日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１１月　８日

出願番号
Application Number: 特願２０００－３４０１５３

出願人
Applicant(s): ソニー株式会社

２００１年１０月２６日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０９４８９９

【書類名】　特許願
【整理番号】　0000571405
【提出日】　平成12年11月 8日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/00
H04L 9/00
【発明者】
【住所又は居所】　東京都品川区東五反田１丁目１４番１０号　株式会社ソニー木原研究所内
【氏名】　大森　睦弘
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代表者】　出井　伸之
【代理人】
【識別番号】　100082131
【弁理士】
【氏名又は名称】　稲本　義雄
【電話番号】　03-3369-6479
【手数料の表示】
【予納台帳番号】　032089
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9708842
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置および方法、記録媒体、並びにサービス提供システム

【特許請求の範囲】

【請求項１】　第１のネットワーク特定情報により特定される、ユーザの個人情報を管理する第１のサーバとともに、所定のネットワークに接続される第２のサーバが、第２のネットワーク特定情報により特定される処理を実行することで、所定のサービスの提供を受ける情報処理装置において、

前記第１のネットワーク特定情報を記憶する記憶手段と、

前記第２のネットワーク特定情報を取得する第１の取得手段と、

前記ユーザを認証するために必要な認証データを取得する第２の取得手段と、

前記第１の取得手段により取得された前記第２のネットワーク特定情報により特定される処理が前記第２のサーバにより実行されることで、前記サービスの提供を受けることができるように、前記記憶手段に記憶されている前記第１のネットワーク特定情報により特定される前記個人情報を管理する前記第１のサーバに、前記第１のネットワーク特定情報および前記第２のネットワーク特定情報を含む制御情報を送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項２】　前記第１のネットワーク特定情報または前記第２のネットワーク特定情報は、ＵＲＬである

ことを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記送信手段は、前記情報処理装置に対する、前記ネットワークのアクセスポートとしてのアクセスポート端末が、前記ネットワークに接続されている場合、前記アクセスポート端末を介して、前記制御情報を、前記第１のサーバに送信する

ことを特徴とする請求項１に記載の情報処理装置。

【請求項４】　前記送信手段は、指向性のある赤外線、または高周波の電波を利用して、前記制御情報を、前記アクセスポート端末に送信する

ことを特徴とする請求項３に記載の情報処理装置。

【請求項５】　前記第２の取得手段は、前記認証データとして、前記ユーザが身に着けている物に組み込まれた認証データ用ＩＣチップが発生するパスワードを取得する

ことを特徴とする請求項１に記載の情報処理装置。

【請求項６】　前記パスワードは、ワンタイムパスワードである

ことを特徴とする請求項５に記載の情報処理装置。

【請求項７】　前記パスワードは、前記情報処理装置と前記第１のサーバとの共通鍵で暗号化されている

ことを特徴とする請求項５に記載の情報処理装置。

【請求項８】　前記パスワードは、前記第１のサーバの公開鍵で暗号化されている

ことを特徴とする請求項５に記載の情報処理装置。

【請求項９】　前記第２の取得手段は、前記第１のサーバからの所定の要求に対して、前記ユーザが身に着けている物に組み込まれた認証データ用ＩＣチップから適切な応答があったとき、前記認証データ用ＩＣチップが発生するパスワードを取得する

ことを特徴とする請求項１に記載の情報処理装置。

【請求項１０】　前記認証データ用ＩＣチップが組み込まれた前記ユーザに身に着けられている物は、腕時計、指輪、または前記認証データ用ＩＣチップに対する防水が施された前記腕時計若しくは前記指輪である

ことを特徴とする請求項５に記載の情報処理装置。

【請求項１１】　前記認証データ用ＩＣチップは、前記情報処理装置からの電磁誘導起電力、光電変換による電力、小型電池からの電力、または前記ユーザの人体からの熱による熱起電力に基づいて動作する

ことを特徴とする請求項５に記載の情報処理装置。

【請求項１２】　前記第２の取得手段は、前記認証データとして、指紋、声紋、虹彩、または人体の特定部分の血管の造影等を取得する

ことを特徴とする請求項５に記載の情報処理装置。

【請求項１３】　前記第１の取得手段は、前記第２のネットワーク特定情報

を、自分自身が有するマイクロフォンにより取り込まれた前記音声、自分自身が有するイメージセンサにより得られた画像、自分自身が有する前記赤外線センサにより受光された赤外線、または自分自身が有する高周波アンテナにより受信された高周波から取得する

ことを特徴とする請求項１に記載の情報処理装置。

【請求項１４】　第１のネットワーク特定情報により特定される、ユーザの個人情報を管理する第１のサーバとともに、所定のネットワークに接続される第２のサーバが、第２のネットワーク特定情報により特定される処理を実行することで、所定のサービスの提供を受ける情報処理装置の情報処理方法において、

前記第１のネットワーク特定情報を記憶する記憶ステップと、

前記第２のネットワーク特定情報を取得する第１の取得ステップと、

前記ユーザを認証するために必要な認証データを取得する第２の取得ステップと、

前記第１の取得ステップの処理で取得された前記第２のネットワーク特定情報により特定される処理が前記第２のサーバにより実行されることで、前記サービスの提供を受けることができるように、前記記憶ステップに記憶されている前記第１のネットワーク特定情報により特定される前記個人情報を管理する前記第１のサーバに、前記第１のネットワーク特定情報および前記第２のネットワーク特定情報を含む制御情報を送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項１５】　第１のネットワーク特定情報により特定される、ユーザの個人情報を管理する第１のサーバとともに、所定のネットワークに接続される第２のサーバが、第２のネットワーク特定情報により特定される処理を実行することで、所定のサービスの提供を受ける情報処理装置のプログラムにおいて、

前記第１のネットワーク特定情報を記憶する記憶ステップと、

前記第２のネットワーク特定情報を取得する第１の取得ステップと、

前記ユーザを認証するために必要な認証データを取得する第２の取得ステップと、

前記第１の取得ステップの処理で取得された前記第２のネットワーク特定情報

により特定される処理が前記第２のサーバにより実行されることで、前記サービスの提供を受けることができるように、前記記憶ステップに記憶されている前記第１のネットワーク特定情報により特定される前記個人情報を管理する前記第１のサーバに、前記第１のネットワーク特定情報および前記第２のネットワーク特定情報を含む制御情報を送信する送信ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項１６】　それぞれネットワークを介して接続される、第１のネットワーク特定情報を保持する携帯端末、前記第１のネットワーク特定情報により特定される、ユーザの個人情報を管理する第１のサーバ、および第２のネットワーク特定情報により特定される処理を実行する第２のサーバからなるサービス提供システムにおいて、

前記携帯端末は、

前記第１のネットワーク特定情報を記憶する第１の記憶手段と、

前記第２のネットワーク特定情報を取得する第１の取得手段と、

前記ユーザを認証するために必要な認証データを取得する第２の取得手段と

前記第１の取得手段により取得された前記第２のネットワーク特定情報により特定される処理が前記第２のサーバにより実行されることで、所定のサービスの提供を受けることができるように、前記第１の記憶手段に記憶されている前記第１のネットワーク特定情報により特定される前記個人情報を管理する前記第１のサーバに、前記第１のネットワーク特定情報および前記第２のネットワーク特定情報を含む制御情報を供給する第１の供給手段と、

前記第２の取得手段により取得された前記認証データを、前記第１のサーバに供給する第２の供給手段と

を備え、

前記第１のサーバは、

前記第１のネットワーク特定情報により特定される前記個人情報を管理する第１の管理手段と、

前記携帯端末の前記第１の供給手段により供給された前記制御情報に含まれる前記第２のネットワーク特定情報により特定される処理を実行する前記第２のサーバに、前記制御情報および前記個人情報に基づく前記サービスの提供を要求する第１の要求手段と、

前記第２のサーバからの要求に基づいて、前記携帯端末の前記第２の供給手段により供給された前記認証データに基づき前記ユーザを認証する第１の認証手段と、

前記第１の認証手段による認証結果を、前記第２のサーバに供給する第３の供給手段と

を備え、

前記第２のサーバは、

前記第２のネットワーク特定情報により特定される処理を管理する第２の管理手段と、

前記第１のサーバの第１の要求手段による要求があったとき、前記ユーザの認証を前記第１のサーバに要求する第２の要求手段と、

前記第１のサーバの第３の供給手段により供給された前記認証結果が、前記ユーザが、前記サービス提供システムの正規のユーザである旨を示しているとき、前記第２のネットワーク特定情報により特定される処理を、前記制御情報および前記個人情報に基づいて実行する第１の実行手段と

を備えることを特徴とするサービス提供システム。

【請求項１７】　前記第１のネットワーク特定情報または前記第２のネットワーク特定情報は、ＵＲＬである

ことを特徴とする請求項１６に記載のサービス提供システム。

【請求項１８】　前記携帯端末に対する、前記ネットワークのアクセスポートとしてのアクセスポート端末が、前記ネットワークにさらに接続されている場合において、

前記携帯端末の前記第１の供給手段または前記第２の供給手段は、前記制御情報または前記認証データを、前記アクセスポート端末に供給し、

前記アクセスポート端末は、前記携帯端末の前記第１の供給手段または前記第

２の供給手段から供給された前記制御情報または前記認証データを、前記第１のサーバに供給する第４の供給手段

を備えることを特徴とする請求項１６に記載のサービス提供システム。

【請求項１９】　前記サービス提供システムの使用料金を決済する第３のサーバが、前記ネットワークにさらに接続されている場合において、

前記アクセスポート端末は、自分自身が処理した所定の通信量を計測するとともに、その計測結果を、前記第３のサーバに供給する第５の供給手段をさらに備え、

前記第３のサーバは、前記アクセスポート端末の前記第５の供給手段から供給された前記計測結果に基づいて、前記サービス提供システムの使用料金を決済する決済手段

を備えることを特徴とする請求項１８に記載のサービス提供システム。

【請求項２０】　前記通信量は、前記アクセスポート端末が、前記携帯端末または前記第１のサーバに転送したデータ量である

ことを特徴とする請求項１９に記載のサービス提供システム。

【請求項２１】　前記携帯端末の、

前記第１の記憶手段は、前記第１のネットワーク特定情報の公開鍵をさらに記憶し、

前記第２の供給手段は、前記第１のネットワーク特定情報の公開鍵を、前記アクセスポート端末にさらに供給し、

前記アクセスポート端末の前記第４の供給手段は、前記携帯端末の前記第２の供給手段により供給された、前記第１のネットワーク特定情報の公開鍵で、前記認証データを暗号化し、暗号化された前記認証データを、前記制御情報とともに、前記第１のサーバに供給し、

前記第１のサーバの、

前記第１の管理手段は、前記第１のネットワーク特定情報の秘密鍵を個人情報としてさらに管理し、

前記第１の認証手段は、前記個人情報に含まれる前記第１のネットワーク特定情報の秘密鍵で、前記アクセスポート端末の前記第４の供給手段から供給さ

れた前記認証データの暗号化を解凍し、暗号化が解凍された前記認証データに基づいて、前記ユーザを認証する

ことを特徴とする請求項１８に記載のサービス提供システム。

【請求項２２】　前記第１のサーバの前記第１の管理手段は、前記第１の認証手段により、前記ユーザが、前記サービス提供システムの正規のユーザであると認証されたとき、前記第１のネットワーク特定情報の秘密鍵を変更し、

前記第１のサーバは、前記第１の管理手段による、前記第１のネットワーク特定情報の秘密鍵の変更に対応させて、前記第１のネットワーク特定情報の公開鍵を変更するように、前記携帯端末に要求する第３の要求手段をさらに備え、

前記携帯端末の前記第１の記憶手段は、前記第１のサーバの前記第３の要求手段による要求に基づいて、前記第１のネットワーク特定情報の公開鍵を変更する

ことを特徴とする請求項２１に記載のサービス提供システム。

【請求項２３】　前記携帯端末の第２の取得手段は、前記ユーザが身に着けた所定の物に組み込まれている認証データ用ＩＣチップが第１のアルゴリズムで発生する、前記認証データとしてのパスワードを取得する

ことを特徴とする請求項１６に記載のサービス提供システム。

【請求項２４】　前記パスワードは、ワンタイムパスワードである

ことを特徴とする請求項２３に記載のサービス提供システム。

【請求項２５】　前記パスワードは、前記携帯端末と前記第１のサーバとの共通鍵で暗号化されている

ことを特徴とする請求項２３に記載のサービス提供システム。

【請求項２６】　前記パスワードは、前記第１のサーバの公開鍵で暗号化されている

ことを特徴とする請求項２３に記載のサービス提供システム。

【請求項２７】　前記携帯端末の第２の取得手段は、前記第１のサーバからの所定の要求に対して、前記ユーザが身に着けている物に組み込まれた認証データ用ＩＣチップから適切な応答があったとき、前記認証データ用ＩＣチップが発生するパスワードを取得する

ことを特徴とする請求項１６に記載のサービス提供システム。

【請求項２８】　前記第１のサーバの前記第１の認証手段は、前記認証データ用ＩＣチップの前記第１のアルゴリズムと同じ第２のアルゴリズムで、前記ワンタイムパスワードを発生し、前記携帯端末の前記第２の供給手段から供給された、前記認証データとしての前記パスワードと照合することによって、前記ユーザを認証する

ことを特徴とする請求項２３に記載のサービス提供システム。

【請求項２９】　前記第１のサーバの前記第１の認証手段は、前記ユーザが、前記サービス提供システムの正規のユーザであると認証したとき、前記第２のアルゴリズムを更新し、

前記第１のサーバは、前記第１の認証手段による、前記第２のアルゴリズムの更新に対応させて、前記認証データ用ＩＣチップの前記第１のアルゴリズムを更新するように、前記携帯端末に要求する第３の要求手段をさらに備え、

前記携帯端末は、前記第１のサーバの前記第３の要求手段による要求に基づいて、前記第１のアルゴリズムを更新するように、前記認証データ用ＩＣチップに要求する第４の要求手段

をさらに備えることを特徴とする請求項２８に記載のサービス提供システム。

【請求項３０】　前記第２のサーバの前記第１の実行手段により、前記第２のネットワーク特定情報により特定される処理が実行されたとき、所定のサービス情報が、前記携帯端末に供給される場合において、

前記第１のサーバの前記第１の管理手段は、前記携帯端末の公開鍵をさらに管理し、

前記第１のサーバは、前記サービス情報を、前記携帯端末の公開鍵で暗号化し、暗号化された前記サービス情報を、前記携帯端末に供給する第４の供給手段

をさらに備え、

前記携帯端末の前記第１の記憶手段は、自分自身の秘密鍵をさらに記憶し、

前記携帯端末は、前記第１のサーバの前記第４の供給手段により供給された前記サービス情報の暗号化を、前記自分自身の秘密鍵で解凍する解凍手段

をさらに備えることを特徴とする請求項１６に記載のサービス提供システム。

【請求項３１】　前記第１のサーバの前記第１の管理手段は、前記第１の認

証手段により、前記ユーザが、前記サービス提供システムの正規のユーザであると認証したとき、前記携帯端末の公開鍵を変更し、

前記第１のサーバは、前記第１の管理手段による、前記携帯端末の公開鍵の変更に対応させて、前記携帯端末の秘密鍵を変更するように、前記携帯端末に要求する第３の要求手段をさらに備え、

前記携帯端末の前記第１の記憶手段は、前記第１のサーバの前記第３の要求手段による要求に基づいて、前記携帯端末の秘密鍵を変更する

ことを特徴とする請求項３０に記載のサービス提供システム。

【請求項３２】　所定のサービス端末がさらに前記ネットワークに接続され、前記第２のネットワーク特定情報により特定される処理が精算処理である場合において、

前記携帯端末の、

前記第１の取得手段は、前記第２のネットワーク特定情報とともに、金額情報を、前記サービス端末から取得し、

前記第１の供給手段は、前記精算処理が前記第２のサーバにより実行されることで、前記金額情報に示される料金の精算を行うことができるように、前記第１のサーバに、前記第１のネットワーク特定情報、前記第２のネットワーク特定情報、および前記金額情報を含む前記制御情報を供給し、

前記第１のサーバの前記第１の要求手段は、前記携帯端末の前記第１の供給手段により供給された前記制御情報に含まれる前記第２のネットワーク特定情報により特定される前記精算処理を実行する前記第２のサーバに、前記金額情報および前記個人情報に基づく精算を行うことを要求し、

前記第２のサーバの前記第１の実行手段は、前記第１のサーバの前記第３の供給手段により供給された前記認証結果が、前記ユーザが、前記サービス提供システムの正規のユーザである旨を示しているとき、前記精算処理を、前記金額情報および前記個人情報に基づいて実行する

ことを特徴とする請求項１６に記載のサービス提供システム。

【請求項３３】　前記携帯端末の、

前記第１の取得手段は、支払ＩＤを、前記サービス端末からさらに取得し、

前記第１の供給手段は、前記支払ＩＤをさらに含む制御情報を、前記第１のサーバに供給し、

前記第１のサーバの前記第１の要求手段は、前記第２のサーバに、前記金額情報、前記個人情報、および前記支払ＩＤに基づく精算を行うことを要求し、

前記第２のサーバの前記第１の実行手段は、前記第１のサーバの前記第３の供給手段により供給された前記認証結果が、前記ユーザが、前記サービス提供システムの正規のユーザである旨を示しているとき、前記精算処理を、前記金額情報、前記個人情報、および前記支払ＩＤに基づいて実行する

ことを特徴とする請求項３２記載のサービス提供システム。

【請求項３４】　前記携帯端末に対する、前記ネットワークのアクセスポートとしてのアクセスポート端末が、前記ネットワークにさらに接続されている場合において、

前記携帯端末の前記第１の供給手段または前記第２の供給手段は、前記制御情報または前記認証データを、前記アクセスポート端末に供給し、

前記アクセスポート端末は、前記携帯端末の前記第１の供給手段または前記第２の供給手段から供給された前記制御情報または前記認証データを、前記第１のサーバに供給する第４の供給手段

を備えることを特徴とする請求項３２に記載のサービス提供システム。

【請求項３５】　前記第１のサーバの第１の管理手段は、前記ユーザの特徴情報をさらに管理し、

前記第１のサーバは、前記第２のサーバからの要求に応じて、前記特徴情報を、前記サービス端末に供給する第５の供給手段をさらに備え、

前記サービス端末は、

前記第１のサーバの前記第５の供給手段により供給された前記特徴情報を利用して、前記ユーザを認証する第２の認証手段と、

前記第２の認証手段による認証結果を、前記第２のサーバに供給する第５の供給手段と

をさらに備え、

前記第２のサーバの前記第１の実行手段は、前記サービス端末の前記第５の供

給手段により供給された前記認識結果が、前記ユーザが、前記サービス提供システムの正規のユーザである旨を示しているとき、前記第２のネットワーク特定情報により特定される処理を、前記制御情報および前記個人情報に基づいて実行する

ことを特徴とする請求項３４に記載のサービス提供システム。

【請求項３６】　前記ユーザの特徴情報は、前記ユーザの顔の部分の画像データであり、

前記サービス端末の前記第２の認証手段による認証は、前記サービス端末の表示部に、前記ユーザの顔の部分の画像データに対応する画像を表示させ、前記サービス端末の管理者が、前記ユーザの実際の顔と、前記画像を照合することで行われる

ことを特徴とする請求項３５に記載のサービス提供システム。

【請求項３７】　前記第２のサーバは、

前記第１のサーバの前記第３の供給手段により供給された前記認証結果に、所定の有効期限を付して記憶する第２の記憶手段と、

前記第１のサーバの前記第１の要求手段による要求に基づいて、前記第２の記憶手段に記憶されている前記認証結果が有効であるか否かを、前記有効期限に基づいて判定する判定手段と

をさらに備え、

前記第２のサーバの前記第１の実行手段は、前記判定手段により、前記認証結果が有効であると判定されたとき、前記第２のネットワーク特定情報により特定される処理を実行する

ことを特徴とする請求項１６に記載のサービス提供システム。

【請求項３８】　所定のチケットを購入することで、通過することができる、ゲートの開閉を制御するサービス端末が、前記ネットワークにさらに接続されている場合において、

前記第１のサーバの前記第３の供給手段は、前記認証手段により、前記ユーザが、前記サービス提供システムの正規のユーザであると認識されたとき、前記認証結果として、前記第１のネットワーク特定情報を、前記第２のサーバに供給し

前記第２のサーバの、

前記第２の記憶手段は、前記第１のサーバの前記第３の供給手段により供給された前記第１のネットワーク特定情報を、前記チケットの発券時に決定された前記有効期限を付して記憶し、

前記判定手段は、前記第１のサーバの前記第１の要求手段による要求に基づいて、前記第２の記憶手段に記憶されている前記第１のネットワーク特定情報が有効であるか否かを、前記有効期限に基づいて判定し、

前記第１の実行手段は、前記判定手段により、前記第１のネットワーク特定情報が有効であると判定されたとき、前記ゲートを開放する処理を実行する

ことを特徴とする請求項３７に記載のサービス提供システム。

【請求項３９】　前記第１のサーバの、

前記第１の管理手段は、前記認証結果を、所定の有効期限を付して管理し、

前記第１の認証手段は、前記第２のサーバの前記第２の要求手段による要求に基づいて、前記認証結果が有効であるか否かを、前記有効期限に基づいて判定し、

前記第３の供給手段は、前記認証結果を、前記第２のサーバに供給し、

前記第２のサーバの、

前記第２の要求手段は、所定のタイミングで、前記ユーザの認証を、前記第１のサーバに要求し、

前記第１の実行手段は、前記第１のサーバの前記第３の供給手段により供給された前記認証結果が、前記認証結果が有効である旨を示しているとき、前記第２のネットワーク特定情報により特定される処理を、前記制御情報および前記個人情報に基づいて実行する

ことを特徴とする請求項１６に記載のサービス提供システム。

【請求項４０】　前記サービス提供システムが、それぞれ異なる前記第２のネットワーク特定情報により特定される処理を実行する１個または複数のサービス処理実行装置をさらに含む場合において、

前記第１のサーバの前記第１の要求手段は、前記第２のサーバおよび前記サー

ビス処理実行装置に、前記制御情報および前記個人情報に基づく前記サービスの提供を要求し、

前記サービス処理実行装置は、それぞれの前記第２のネットワーク特定情報により特定される処理を実行する第２の実行手段

を備えることを特徴とする請求項１６に記載のサービス提供システム。

【請求項４１】　前記サービス処理実行装置の前記第２の実行手段は、パーソナルコンピュータを構成する、モニタ、マウス、またはキーボードとしての処理を実行し、

前記第２のサーバは、前記パーソナルコンピュータを構成するＣＰＵとしての処理を実行する

ことを特徴とする請求項４０に記載のサービス提供システム。

【請求項４２】　前記携帯端末は、前記第１のネットワーク特定情報を、１個または複数の前記サービス処理実行装置に供給する第４の供給手段

をさらに備え、

前記１個または複数のサービス処理実行装置の前記第２の実行手段は、前記携帯端末の前記第４の供給手段により、前記第１のネットワーク特定情報が供給されたときにのみ、前記第２のネットワーク特定情報により特定される処理を実行する

ことを特徴とする請求項４０に記載のサービス提供システム。

【請求項４３】　１個の前記サービス処理実行装置の前記第２の実行手段が、前記キーボードとしての処理を実行し、前記第２のサーバが、文章作成処理を実行している場合において、

前記第１のサーバの、

前記第１の管理手段は、前記キーボードに対する前記ユーザに対する、文字入力パターンを含む前記個人情報を管理し、

前記第１の要求手段は、前記携帯端末の前記第１の供給手段により供給された前記制御情報に含まれる前記第２のネットワーク特定情報により特定される処理を実行する前記第２のサーバに、前記制御情報、および前記文字入力パターンに基づく前記文書作成処理の実行を要求し、

前記第２のサーバの前記第１の実行手段は、前記制御情報および前記文字入力パターンに基づいて前記文章作成処理を実行する

ことを特徴とする請求項４０に記載のサービス提供システム。

【請求項４４】　前記第２のサーバの前記第１の実行手段により、前記第２のネットワーク特定情報により特定される処理が実行された結果、前記携帯端末が所定のサービス情報の提供を受ける場合において、

前記携帯端末は、

前記サービス情報を一時的に記憶する第２の記憶手段と、

前記第２の記憶手段に記憶されている前記サービス情報のデータ量を監視し

所定のデータ量以上の前記サービス情報が記憶されたとき、ブックマークが付されていない前記サービス情報、または前記ブックマークが付されたホームページとリンクされていない前記サービス情報を、優先的に削除する削除手段とをさらに備えることを特徴とする請求項１６に記載のサービス提供システム。

【請求項４５】　前記削除手段は、前記ブックマークに優先順位を設け、必要に応じて、前記優先順位に従って、前記ブックマークに付された前記サービス情報を削除する

ことを特徴とする請求項４４に記載のサービス提供システム。

【請求項４６】　前記サービス情報が、前記個人情報である場合、前記第１のサーバは、前記個人情報に、前記個人情報が前記携帯端末の前記第２の記憶手段に記憶することができないものであることを示すタグを付して、前記携帯端末に供給する第４の供給手段

をさらに備えることを特徴とする請求項４５に記載のサービス提供システム。

【請求項４７】　前記第２のサーバの前記第１の実行手段により、前記第２のネットワーク特定情報により特定される処理が実行された結果、前記第１のサーバが所定のサービス情報の提供を受ける場合において、

前記第１のサーバは、

前記サービス情報を一時的に記憶する第２の記憶手段と、

前記第２の記憶手段に記憶されている前記サービス情報のデータ量を監視し

所定のデータ量以上の前記サービス情報が記憶されたとき、ブックマークが付されていない前記サービス情報、または前記ブックマークが付されたホームページとリンクされていない前記サービス情報を、優先的に削除する削除手段とをさらに備えることを特徴とする請求項１６に記載のサービス提供システム。

【請求項４８】　前記削除手段は、前記ブックマークに優先順位を設け、必要に応じて、前記優先順位に従って、前記ブックマークに付された前記サービス情報を削除する

ことを特徴とする請求項４７に記載のサービス提供システム。

【請求項４９】　前記第２のネットワーク特定情報により特定される処理が、ウエブブラウジングのための処理である場合、前記第１のサーバの前記第１の管理手段は、一度閲覧したホームページを再度閲覧するのに有効な所定の情報をさらに管理する

ことを特徴とする請求項１６に記載のサービス提供システム。

【請求項５０】　それぞれネットワークを介して接続される、第１のネットワーク特定情報を保持する携帯端末、前記第１のネットワーク特定情報により特定される、ユーザの個人情報を管理する第１のサーバ、第２のネットワーク特定情報により特定される処理を実行する第２のサーバ、前記第２のネットワーク特定情報を保持するサービス端末からなるサービス提供システムにおいて、

前記携帯端末は、

前記第１のネットワーク特定情報を記憶する記憶手段と、

前記第２のネットワーク特定情報およびアクセスパターン検出のためのアクセス情報を、前記サービス端末から取得する第１の取得手段と、

前記第１の取得手段により取得された前記第２のネットワーク特定情報により特定される処理が前記第２のサーバにより実行されることで、所定のサービスの提供を受けることができるように、前記記憶手段に記憶されている前記第１のネットワーク特定情報により特定される前記個人情報を管理する前記第１のサーバに、前記第１のネットワーク特定情報、前記第２のネットワーク特定情報、および前記アクセス情報を含む制御情報を、前記サービス端末に供給す

る第１の供給手段と

を備え、

前記サービス端末は、

前記第２のネットワーク特定情報を保持する第１の保持手段と、

前記携帯端末の前記第１の取得手段による自分自身に対するアクセスから、前記アクセス情報を取得する第２の取得手段と、

前記携帯端末の前記第１の取得手段により取得されるように、前記第２のネットワーク特定情報および前記アクセス情報を、前記携帯端末に供給する第２の供給手段と、

前記携帯端末の前記第１の供給手段により供給された前記制御情報を、前記第１のサーバに供給する第３の供給手段と

を備え、

前記第１のサーバは、

前記第１のネットワーク特定情報により特定される前記個人情報を管理する第１の管理手段と、

前記サービス端末の前記第２の供給手段により供給された前記制御情報に含まれる前記第２のネットワーク特定情報により特定される処理を実行する前記第２のサーバに、前記制御情報、前記個人情報、および前記アクセス情報に基づく前記サービスの提供を要求する第１の要求手段と

を備え、

前記第２のサーバは、

前記第２のネットワーク特定情報により特定される処理を管理する第２の管理手段と、

前記第１のサーバの前記第１の要求手段による要求に基づいて、前記第２のネットワーク特定情報により特定される前記処理を、前記制御情報、前記個人情報、および前記アクセス情報に基づいて実行する実行手段と

を備えることを特徴とするサービス提供システム。

【請求項５１】　第１の前記サービス端末が、第１の場所に設けられ、第２の前記サービス端末が、第２の場所に設けられ、前記携帯端末の前記第１の取得

手段は、前記第１のサービス端末に先にアクセスし、その後、前記第２のサービス端末にアクセスする場合において、

前記アクセス情報は、アクセスされた時刻を含み、

前記第２のサーバの実行手段は、前記第１のサービス端末の前記第１の取得手段により取得された前記アクセス情報に含まれる前記時刻と、前記第２のサービス端末の前記第１の取得手段により取得された前記アクセス情報に含まれる時刻との差分を算出するとともに、その算出結果が、所定の時間以上であるか否かを判定し、前記時間以上であると判定した場合、前記第２のネットワーク特定情報により特定される処理を実行する

ことを特徴とする請求項５０に記載のサービス提供システム。

【請求項５２】　前記第１の場所および前記第２の場所は、遊園地の通路の所定の場所または有料道路の入口若しくは出口付近の所定の場所である

ことを特徴とする請求項５１に記載のサービス提供システム。

【請求項５３】　前記第１の場所が、前記有料道路の入口付近の所定の場所であり、前記第２の場所が、前記有料道路の出口付近の所定の場所である場合において、

前記第２のサービス端末は、

通過する車両を撮像する撮像手段と、

前記撮像手段による撮像結果から、前記車両の前記車両番号を取得する第３の取得手段と

を備え、

前記第２のサービス端末の前記第３の供給手段は、前記第３の取得手段により取得された前記車両番号を、前記第１のサーバにさらに供給し、

前記第１のサーバの前記第１の要求手段は、前記第２のサービス端末の前記第３の供給手段により供給された前記制御情報に含まれる前記第２のネットワーク特定情報により特定される処理を実行する前記第２のサーバに、前記制御情報、前記個人情報、前記アクセス情報、および前記第２のサービス端末の前記第２の取得手段により取得された前記車両番号に基づく前記サービスの提供を要求し、

前記第２のサーバは、前記ユーザの車両の車両番号を予め保持する第２の保持

手段をさらに備え、

前記第２のサーバの前記実行手段は、前記第２のサービス端末の前記第２の取得手段により取得された前記車両番号が、前記第２の保持手段により保持されている前記車両番号と一致するか否かを判定し、一致すると判定した場合、前記有料道路の通行料金の精算処理を、前記制御情報および前記個人情報に基づいて実行する

ことを特徴とする請求項５２に記載のサービス提供システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置、情報処理方法、および記録媒体、並びにサービス提供システムに関し、特に、例えば、ユーザが利用する端末を紛失しても、安全に利用することができるようにした情報処理装置、情報処理方法、および記録媒体、並びにサービス提供システムに関する。

【０００２】

【従来の技術】

ユーザが携帯端末を操作し、所定のネットワークに接続されているサーバと通信を行うことで、そのサーバから、所定のサービスの提要を受けることができるサービス提供システムが存在する。

【０００３】

【発明が解決しようとする課題】

しかしながら、通常、この携帯端末に、サービス提供システムを利用するために必要なユーザＩＤやユーザ認証のためのパスワードなどの個人情報が記憶されているようになされている。すなわち、例えば、携帯端末を紛失した場合、それらの個人情報が悪用されてしまう課題があった。

【０００４】

また、個人情報を送受信する場合、その漏洩を防止するために、携帯端末において暗号化がされる場合もあるが、通常の携帯端末の機能では、高度な暗号化を行うことができない。すなわち、個人情報が解読され、漏洩する課題があった。

【０００５】

さらに、携帯端末として携帯電話を利用することもできるが、携帯電話の使用は、例えば、心臓ペースメーカ等の医療用の精密機器への影響を考慮して、場所によって制限されている。すなわち、このシステムの利用が制限されてしまう課題があった。

【０００６】

以上のように、従来のサービス提供システムでは、その利用に多くの制限が課される課題があった。

【０００７】

本発明はこのような状況に鑑みてなされたものであり、ユーザに多くの制限を課すことなく、サービス提供システムを利用することができるようにするものである。

【０００８】

【課題を解決するための手段】

本発明の情報処理装置は、第１のネットワーク特定情報を記憶する記憶手段と、第２のネットワーク特定情報を取得する第１の取得手段と、ユーザを認証するために必要な認証データを取得する第２の取得手段と、第１の取得手段により取得された第２のネットワーク特定情報により特定される処理が第２のサーバにより実行されることで、サービスの提供を受けることができるように、記憶手段に記憶されている第１のネットワーク特定情報により特定される個人情報を管理する第１のサーバに、第１のネットワーク特定情報および第２のネットワーク特定情報を含む制御情報を送信する送信手段とを備えることを特徴とする。

【０００９】

第１のネットワーク特定情報または第２のネットワーク特定情報は、ＵＲＬとすることができる。

【００１０】

送信手段は、情報処理装置に対する、ネットワークのアクセスポートとしてのアクセスポート端末が、ネットワークに接続されている場合、アクセスポート端末を介して、制御情報を、第１のサーバに送信することができる。

【００１１】

送信手段は、指向性のある赤外線、または高周波の電波を利用して、制御情報を、アクセスポート端末に送信することができる。

【００１２】

第２の取得手段は、認証データとして、ユーザが身に着けている物に組み込まれた認証データ用ＩＣチップが発生するパスワードを取得することができる。

【００１３】

パスワードは、ワンタイムパスワードとすることができる。

【００１４】

パスワードは、情報処理装置と第１のサーバとの共通鍵で暗号化されているものとすることができる。

【００１５】

パスワードは、第１のサーバの公開鍵で暗号化されているものとすることができる。

【００１６】

第２の取得手段は、第１のサーバからの所定の要求に対して、ユーザが身に着けている物に組み込まれた認証データ用ＩＣチップから適切な応答があったとき、認証データ用ＩＣチップが発生するパスワードを取得することができる。

【００１７】

認証データ用ＩＣチップが組み込まれたユーザに身に着けられている物は、腕時計、指輪、または認証データ用ＩＣチップに対する防水が施された腕時計若しくは指輪とすることができる。

【００１８】

認証データ用ＩＣチップは、情報処理装置からの電磁誘導起電力、光電変換による電力、小型電池からの電力、またはユーザの人体からの熱による熱起電力に基づいて動作することができる。

【００１９】

第２の取得手段は、認証データとして、指紋、声紋、虹彩、または人体の特定部分の血管の造影等を取得することができる。

【００２０】

第１の取得手段は、第２のネットワーク特定情報を、自分自身が有するマイクロフォンにより取り込まれた音声、自分自身が有するイメージセンサにより得られた画像、自分自身が有する赤外線センサにより受光された赤外線、または自分自身が有する高周波アンテナにより受信された高周波から取得することができる。

【００２１】

本発明の情報処理方法は、第１のネットワーク特定情報を記憶する記憶ステップと、第２のネットワーク特定情報を取得する第１の取得ステップと、ユーザを認証するために必要な認証データを取得する第２の取得ステップと、第１の取得ステップの処理で取得された第２のネットワーク特定情報により特定される処理が第２のサーバにより実行されることで、サービスの提供を受けることができるように、記憶ステップに記憶されている第１のネットワーク特定情報により特定される個人情報を管理する第１のサーバに、第１のネットワーク特定情報および第２のネットワーク特定情報を含む制御情報を送信する送信ステップとを含むことを特徴とする。

【００２２】

本発明の記録媒体のプログラムは、第１のネットワーク特定情報を記憶する記憶ステップと、第２のネットワーク特定情報を取得する第１の取得ステップと、ユーザを認証するために必要な認証データを取得する第２の取得ステップと、第１の取得ステップの処理で取得された第２のネットワーク特定情報により特定される処理が第２のサーバにより実行されることで、サービスの提供を受けることができるように、記憶ステップに記憶されている第１のネットワーク特定情報により特定される個人情報を管理する第１のサーバに、第１のネットワーク特定情報および第２のネットワーク特定情報を含む制御情報を送信する送信ステップとを含むことを特徴とする。

【００２３】

本発明の情報処理装置および方法、並びに記録媒体のプログラムにおいては、第１のネットワーク特定情報が記憶され、第２のネットワーク特定情報が取得さ

れ、ユーザを認証するために必要な認証データが取得され、取得された第２のネットワーク特定情報により特定される処理が第２のサーバにより実行されることで、サービスの提供を受けることができるように、記憶されている第１のネットワーク特定情報により特定される個人情報を管理する第１のサーバに、第１のネットワーク特定情報および第２のネットワーク特定情報を含む制御情報が送信される。

【００２４】

本発明の第１のサービス提供システムは、携帯端末が、第１のネットワーク特定情報を記憶する第１の記憶手段と、第２のネットワーク特定情報を取得する第１の取得手段と、ユーザを認証するために必要な認証データを取得する第２の取得手段と、第１の取得手段により取得された第２のネットワーク特定情報により特定される処理が第２のサーバにより実行されることで、所定のサービスの提供を受けることができるように、第１の記憶手段に記憶されている第１のネットワーク特定情報により特定される個人情報を管理する第１のサーバに、第１のネットワーク特定情報および第２のネットワーク特定情報を含む制御情報を供給する第１の供給手段と、第２の取得手段により取得された認証データを、第１のサーバに供給する第２の供給手段とを備え、第１のサーバが、第１のネットワーク特定情報により特定される個人情報を管理する第１の管理手段と、携帯端末の第１の供給手段により供給された制御情報に含まれる第２のネットワーク特定情報により特定される処理を実行する第２のサーバに、制御情報および個人情報に基づくサービスの提供を要求する第１の要求手段と、第２のサーバからの要求に基づいて、携帯端末の第２の供給手段により供給された認証データに基づきユーザを認証する第１の認証手段と、第１の認証手段による認証結果を、第２のサーバに供給する第３の供給手段とを備え、第２のサーバが、第２のネットワーク特定情報により特定される処理を管理する第２の管理手段と、第１のサーバの第１の要求手段による要求があったとき、ユーザの認証を第１のサーバに要求する第２の要求手段と、第１のサーバの第３の供給手段により供給された認証結果が、ユーザが、第１のサービス提供システムの正規のユーザである旨を示しているとき、第２のネットワーク特定情報により特定される処理を、制御情報および個人情報

に基づいて実行する第１の実行手段とを備えることを特徴とする。

【００２５】

第１のネットワーク特定情報または第２のネットワーク特定情報は、ＵＲＬとすることができる。

【００２６】

携帯端末に対する、ネットワークのアクセスポートとしてのアクセスポート端末が、ネットワークにさらに接続されている場合において、携帯端末の第１の供給手段または第２の供給手段は、制御情報または認証データを、アクセスポート端末に供給し、アクセスポート端末は、携帯端末の第１の供給手段または第２の供給手段から供給された制御情報または認証データを、第１のサーバに供給する第４の供給手段を設けることができる。

【００２７】

第１のサービス提供システムの使用料金を決済する第３のサーバが、ネットワークにさらに接続されている場合において、アクセスポート端末には、自分自身が処理した所定の通信量を計測するとともに、その計測結果を、第３のサーバに供給する第５の供給手段をさらに設け、第３のサーバには、アクセスポート端末の第５の供給手段から供給された計測結果に基づいて、第１のサービス提供システムの使用料金を決済する決済手段を設けることができる。

【００２８】

通信量は、アクセスポート端末が、携帯端末または第１のサーバに転送したデータ量とすることができる。

【００２９】

携帯端末の、第１の記憶手段は、第１のネットワーク特定情報の公開鍵をさらに記憶し、第２の供給手段は、第１のネットワーク特定情報の公開鍵を、アクセスポート端末にさらに供給し、アクセスポート端末の第４の供給手段は、携帯端末の第２の供給手段により供給された、第１のネットワーク特定情報の公開鍵で、認証データを暗号化し、暗号化された認証データを、制御情報とともに、第１のサーバに供給し、第１のサーバの、第１の管理手段は、第１のネットワーク特定情報の秘密鍵を個人情報としてさらに管理し、第１の認証手段は、個人情報に

含まれる第１のネットワーク特定情報の秘密鍵で、アクセスポート端末の第４の供給手段から供給された認証データの暗号化を解凍し、暗号化が解凍された認証データに基づいて、ユーザを認証することができる。

【００３０】

第１のサーバの第１の管理手段は、第１の認証手段により、ユーザが、第１のサービス提供システムの正規のユーザであると認証されたとき、第１のネットワーク特定情報の秘密鍵を変更し、第１のサーバには、第１の管理手段による、第１のネットワーク特定情報の秘密鍵の変更に対応させて、第１のネットワーク特定情報の公開鍵を変更するように、携帯端末に要求する第３の要求手段をさらに設け、携帯端末の第１の記憶手段は、第１のサーバの第３の要求手段による要求に基づいて、第１のネットワーク特定情報の公開鍵を変更することができる。

【００３１】

携帯端末の第２の取得手段は、ユーザが身に着けた所定の物に組み込まれている認証データ用ＩＣチップが第１のアルゴリズムで発生する、認証データとしてのパスワードを取得することができる。

【００３２】

パスワードは、ワンタイムパスワードとすることができる。

【００３３】

パスワードは、携帯端末と第１のサーバとの共通鍵で暗号化されているものとすることができる。

【００３４】

パスワードは、第１のサーバの公開鍵で暗号化されているものとすることができる。

【００３５】

携帯端末の第２の取得手段は、第１のサーバからの所定の要求に対して、ユーザが身に着けている物に組み込まれた認証データ用ＩＣチップから適切な応答があったとき、認証データ用ＩＣチップが発生するパスワードを取得することができる。

【００３６】

第１のサーバの第１の認証手段は、認証データ用ＩＣチップの第１のアルゴリズムと同じ第２のアルゴリズムで、ワンタイムパスワードを発生し、携帯端末の第２の供給手段から供給された、認証データとしてのパスワードと照合することによって、ユーザを認証することができる。

【００３７】

第１のサーバの第１の認証手段は、ユーザが、第１のサービス提供システムの正規のユーザであると認証したとき、第２のアルゴリズムを更新し、第１のサーバには、第１の認証手段による、第２のアルゴリズムの更新に対応させて、認証データ用ＩＣチップの第１のアルゴリズムを更新するように、携帯端末に要求する第３の要求手段をさらに設け、携帯端末には、第１のサーバの第３の要求手段による要求に基づいて、第１のアルゴリズムを更新するように、認証データ用ＩＣチップに要求する第４の要求手段をさらに設けることができる。

【００３８】

第２のサーバの第１の実行手段により、第２のネットワーク特定情報により特定される処理が実行されたとき、所定のサービス情報が、携帯端末に供給される場合において、第１のサーバの第１の管理手段は、携帯端末の公開鍵をさらに管理し、第１のサーバには、サービス情報を、携帯端末の公開鍵で暗号化し、暗号化されたサービス情報を、携帯端末に供給する第４の供給手段をさらに設け、携帯端末の第１の記憶手段は、自分自身の秘密鍵をさらに記憶し、携帯端末は、第１のサーバの第４の供給手段により供給されたサービス情報の暗号化を、自分自身の秘密鍵で解凍する解凍手段をさらに設けることができる。

【００３９】

第１のサーバの第１の管理手段は、第１の認証手段により、ユーザが、第１のサービス提供システムの正規のユーザであると認証したとき、携帯端末の公開鍵を変更し、第１のサーバには、第１の管理手段による、携帯端末の公開鍵の変更に対応させて、携帯端末の秘密鍵を変更するように、携帯端末に要求する第３の要求手段をさらに設け、携帯端末の第１の記憶手段は、第１のサーバの第３の要求手段による要求に基づいて、携帯端末の秘密鍵を変更することができる。

【００４０】

所定のサービス端末がさらにネットワークに接続され、第２のネットワーク特定情報により特定される処理が精算処理である場合において、携帯端末の、第１の取得手段は、第２のネットワーク特定情報とともに、金額情報を、サービス端末から取得し、第１の供給手段は、精算処理が第２のサーバにより実行されることで、金額情報に示される料金の精算を行うことができるように、第１のサーバに、第１のネットワーク特定情報、第２のネットワーク特定情報、および金額情報を含む制御情報を供給し、第１のサーバの第１の要求手段は、携帯端末の第１の供給手段により供給された制御情報に含まれる第２のネットワーク特定情報により特定される精算処理を実行する第２のサーバに、金額情報および個人情報に基づく精算を行うことを要求し、第２のサーバの第１の実行手段は、第１のサーバの第３の供給手段により供給された認証結果が、ユーザが、第１のサービス提供システムの正規のユーザである旨を示しているとき、精算処理を、金額情報および個人情報に基づいて実行することができる。

【００４１】

携帯端末の、第１の取得手段は、支払ＩＤを、サービス端末からさらに取得し、第１の供給手段は、支払ＩＤをさらに含む制御情報を、第１のサーバに供給し、第１のサーバの第１の要求手段は、第２のサーバに、金額情報、個人情報、および支払ＩＤに基づく精算を行うことを要求し、第２のサーバの第１の実行手段は、第１のサーバの第３の供給手段により供給された認証結果が、ユーザが、第１のサービス提供システムの正規のユーザである旨を示しているとき、精算処理を、金額情報、個人情報、および支払ＩＤに基づいて実行することができる。

【００４２】

携帯端末に対する、ネットワークのアクセスポートとしてのアクセスポート端末が、ネットワークにさらに接続されている場合において、携帯端末の第１の供給手段または第２の供給手段は、制御情報または認証データを、アクセスポート端末に供給し、アクセスポート端末には、携帯端末の第１の供給手段または第２の供給手段から供給された制御情報または認証データを、第１のサーバに供給する第４の供給手段を設けることができる。

【００４３】

第１のサーバの第１の管理手段は、ユーザの特徴情報をさらに管理し、第１のサーバには、第２のサーバからの要求に応じて、特徴情報を、サービス端末に供給する第５の供給手段をさらに設け、サービス端末には、第１のサーバの第５の供給手段により供給された特徴情報を利用して、ユーザを認証する第２の認証手段と、第２の認証手段による認証結果を、第２のサーバに供給する第５の供給手段とをさらに設け、第２のサーバの第１の実行手段は、サービス端末の第５の供給手段により供給された認識結果が、ユーザが、第１のサービス提供システムの正規のユーザである旨を示しているとき、第２のネットワーク特定情報により特定される処理を、制御情報および個人情報に基づいて実行することができる。

【００４４】

ユーザの特徴情報は、ユーザの顔の部分の画像データであり、サービス端末の第２の認証手段による認証は、サービス端末の表示部に、ユーザの顔の部分の画像データに対応する画像を表示させ、サービス端末の管理者が、ユーザの実際の顔と、画像を照合することで行われるようにすることができる。

【００４５】

第２のサーバには、第１のサーバの第３の供給手段により供給された認証結果に、所定の有効期限を付して記憶する第２の記憶手段と、第１のサーバの第１の要求手段による要求に基づいて、第２の記憶手段に記憶されている認証結果が有効であるか否かを、有効期限に基づいて判定する判定手段とをさらに設け、第２のサーバの第１の実行手段は、判定手段により、認証結果が有効であると判定されたとき、第２のネットワーク特定情報により特定される処理を実行することができる。

【００４６】

所定のチケットを購入することで、通過することができる、ゲートの開閉を制御するサービス端末が、ネットワークにさらに接続されている場合において、第１のサーバの第３の供給手段は、認証手段により、ユーザが、第１のサービス提供システムの正規のユーザであると認識されたとき、認証結果として、第１のネットワーク特定情報を、第２のサーバに供給し、第２のサーバの、第２の記憶手段は、第１のサーバの第３の供給手段により供給された第１のネットワーク特定

情報を、チケットの発券時に決定された有効期限を付して記憶し、判定手段は、第１のサーバの第１の要求手段による要求に基づいて、第２の記憶手段に記憶されている第１のネットワーク特定情報が有効であるか否かを、有効期限に基づいて判定し、第１の実行手段は、判定手段により、第１のネットワーク特定情報が有効であると判定されたとき、ゲートを開放する処理を実行することができる。

【００４７】

第１のサーバの、第１の管理手段は、認証結果を、所定の有効期限を付して管理し、第１の認証手段は、第２のサーバの第２の要求手段による要求に基づいて、認証結果が有効であるか否かを、有効期限に基づいて判定し、第３の供給手段は、認証結果を、第２のサーバに供給し、第２のサーバの、第２の要求手段は、所定のタイミングで、ユーザの認証を、第１のサーバに要求し、第１の実行手段は、第１のサーバの第３の供給手段により供給された認証結果が、認証結果が有効である旨を示しているとき、第２のネットワーク特定情報により特定される処理を、制御情報および個人情報に基づいて実行することができる。

【００４８】

第１のサービス提供システムが、それぞれ異なる第２のネットワーク特定情報により特定される処理を実行する１個または複数のサービス処理実行装置をさらに含む場合において、第１のサーバの第１の要求手段は、第２のサーバおよびサービス処理実行装置に、制御情報および個人情報に基づくサービスの提供を要求し、サービス処理実行装置には、それぞれの第２のネットワーク特定情報により特定される処理を実行する第２の実行手段を設けることができる。

【００４９】

サービス処理実行装置の第２の実行手段は、パーソナルコンピュータを構成する、モニタ、マウス、またはキーボードとしての処理を実行し、第２のサーバは、パーソナルコンピュータを構成するＣＰＵとしての処理を実行することができる。携帯端末には、第１のネットワーク特定情報を、１個または複数のサービス処理実行装置に供給する第４の供給手段をさらに設け、１個または複数のサービス処理実行装置の第２の実行手段は、携帯端末の第４の供給手段により、第１のネットワーク特定情報が供給されたときにのみ、第２のネットワーク特定情報に

より特定される処理を実行することができる。

【００５０】

１個のサービス処理実行装置の第２の実行手段が、キーボードとしての処理を実行し、第２のサーバが、文章作成処理を実行している場合において、第１のサーバの、第１の管理手段は、キーボードに対するユーザに対する、文字入力パターンを含む個人情報を管理し、第１の要求手段は、携帯端末の第１の供給手段により供給された制御情報に含まれる第２のネットワーク特定情報により特定される処理を実行する第２のサーバに、制御情報、および文字入力パターンに基づく文書作成処理の実行を要求し、第２のサーバの第１の実行手段は、制御情報および文字入力パターンに基づいて文章作成処理を実行することができる。

【００５１】

第２のサーバの第１の実行手段により、第２のネットワーク特定情報により特定される処理が実行された結果、携帯端末が所定のサービス情報の提供を受ける場合において、携帯端末には、サービス情報を一時的に記憶する第２の記憶手段と、第２の記憶手段に記憶されているサービス情報のデータ量を監視し、所定のデータ量以上のサービス情報が記憶されたとき、ブックマークが付されていないサービス情報、またはブックマークが付されたホームページとリンクされていないサービス情報を、優先的に削除する削除手段とをさらに設けることができる。

【００５２】

削除手段は、ブックマークに優先順位を設け、必要に応じて、優先順位に従って、ブックマークに付されたサービス情報を削除することができる。

【００５３】

サービス情報が、個人情報である場合、第１のサーバには、個人情報に、個人情報が携帯端末の第２の記憶手段に記憶することができないものであることを示すタグを付して、携帯端末に供給する第４の供給手段をさらに設けることができる。

【００５４】

第２のサーバの第１の実行手段により、第２のネットワーク特定情報により特定される処理が実行された結果、第１のサーバが所定のサービス情報の提供を受

ける場合において、第１のサーバには、サービス情報を一時的に記憶する第２の記憶手段と、第２の記憶手段に記憶されているサービス情報のデータ量を監視し、所定のデータ量以上のサービス情報が記憶されたとき、ブックマークが付されていないサービス情報、またはブックマークが付されたホームページとリンクされていないサービス情報を、優先的に削除する削除手段とをさらに設けることができる。

【００５５】

削除手段は、ブックマークに優先順位を設け、必要に応じて、優先順位に従って、ブックマークに付されたサービス情報を削除することができる。

【００５６】

第２のネットワーク特定情報により特定される処理が、ウエブブラウジングのための処理である場合、第１のサーバの第１の管理手段は、一度閲覧したホームページを再度閲覧するのに有効な所定の情報をさらに管理することができる。

【００５７】

本発明の第１のサービス提供システムにおいては、携帯端末で、第１のネットワーク特定情報が記憶され、第２のネットワーク特定情報が取得され、ユーザを認証するために必要な認証データが取得され、取得された第２のネットワーク特定情報により特定される処理が第２のサーバにより実行されることで、所定のサービスの提供を受けることができるように、記憶されている第１のネットワーク特定情報により特定される個人情報を管理する第１のサーバに、第１のネットワーク特定情報および第２のネットワーク特定情報を含む制御情報が供給され、取得された認証データが、第１のサーバに供給され、第１のサーバで、第１のネットワーク特定情報により特定される個人情報が管理され、供給された制御情報に含まれる第２のネットワーク特定情報により特定される処理を実行する第２のサーバに、制御情報および個人情報に基づくサービスの提供が要求され、第２のサーバからの要求に基づいて、供給された認証データに基づきユーザが認証され、認証結果が、第２のサーバに供給され、第２のサーバで、第２のネットワーク特定情報により特定される処理が管理され、要求があったとき、ユーザの認証が第１のサーバに要求され、供給された認証結果が、ユーザが、サービス提供システ

ムの正規のユーザである旨を示しているとき、第２のネットワーク特定情報により特定される処理が、制御情報および個人情報に基づいて実行される。

【００５８】

本発明の第２のサービス提供システムは、携帯端末が、第１のネットワーク特定情報を記憶する記憶手段と、第２のネットワーク特定情報およびアクセスパターン検出のためのアクセス情報を、サービス端末から取得する第１の取得手段と、第１の取得手段により取得された第２のネットワーク特定情報により特定される処理が第２のサーバにより実行されることで、所定のサービスの提供を受けることができるように、記憶手段に記憶されている第１のネットワーク特定情報により特定される個人情報を管理する第１のサーバに、第１のネットワーク特定情報、第２のネットワーク特定情報、およびアクセス情報を含む制御情報を、サービス端末に供給する第１の供給手段とを備え、サービス端末が、第２のネットワーク特定情報を保持する第１の保持手段と、携帯端末の第１の取得手段による自分自身に対するアクセスから、アクセス情報を取得する第２の取得手段と、携帯端末の第１の取得手段により取得されるように、第２のネットワーク特定情報およびアクセス情報を、携帯端末に供給する第２の供給手段と、携帯端末の第１の供給手段により、制御情報が供給された制御情報を、第１のサーバに供給する第３の供給手段とを備え、第１のサーバが、第１のネットワーク特定情報により特定される個人情報を管理する第１の管理手段と、サービス端末の第２の供給手段により供給された制御情報に含まれる第２のネットワーク特定情報により特定される処理を実行する第２のサーバに、制御情報、個人情報、およびアクセス情報に基づくサービスの提供を要求する第１の要求手段とを備え、第２のサーバが、第２のネットワーク特定情報により特定される処理を管理する第２の管理手段と、第１のサーバの第１の要求手段による要求に基づいて、第２のネットワーク特定情報により特定される処理を、制御情報、個人情報、およびアクセス情報に基づいて実行する実行手段とを備えることを特徴とする。

【００５９】

第１のサービス端末が、第１の場所に設けられ、第２のサービス端末が、第２の場所に設けられ、携帯端末の第１の取得手段は、第１のサービス端末に先にア

クセスし、その後、第２のサービス端末にアクセスする場合において、アクセス情報は、アクセスされた時刻を含み、第２のサーバの実行手段は、第１のサービス端末の第１の取得手段により取得されたアクセス情報に含まれる時刻と、第２のサービス端末の第１の取得手段により取得されたアクセス情報に含まれる時刻との差分を算出するとともに、その算出結果が、所定の時間以上であるか否かを判定し、時間以上であると判定した場合、第２のネットワーク特定情報により特定される処理を実行することができる。

【００６０】

第１の場所および第２の場所は、遊園地の通路の所定の場所または有料道路の入口若しくは出口付近の所定の場所とすることができる。

【００６１】

第１の場所が、有料道路の入口付近の所定の場所であり、第２の場所が、有料道路の出口付近の所定の場所である場合において、第２のサービス端末には、通過する車両を撮像する撮像手段と、撮像手段による撮像結果から、車両の車両番号を取得する第３の取得手段とを設け、第２のサービス端末の第３の供給手段は、第３の取得手段により取得された車両番号を、第１のサーバにさらに供給し、第１のサーバの第１の要求手段は、第２のサービス端末の第３の供給手段により供給された制御情報に含まれる第２のネットワーク特定情報により特定される処理を実行する第２のサーバに、制御情報、個人情報、アクセス情報、および第２のサービス端末の第２の取得手段により取得された車両番号に基づくサービスの提供を要求し、第２のサーバには、ユーザの車両の車両番号を予め保持する第２の保持手段をさらに設け、第２のサーバの実行手段は、第２のサービス端末の第２の取得手段により取得された車両番号が、第２の保持手段により保持されている車両番号と一致するか否かを判定し、一致すると判定した場合、有料道路の通行料金の精算処理を、制御情報および個人情報に基づいて実行することができる。

【００６２】

本発明の第２のサービス提供システムにおいては、携帯端末で、第１のネットワーク特定情報が記憶され、第２のネットワーク特定情報およびアクセスパター

ン検出のためのアクセス情報が、サービス端末から取得され、取得された第２のネットワーク特定情報により特定される処理が第２のサーバにより実行されることで、所定のサービスの提供を受けることができるように、記憶されている第１のネットワーク特定情報により特定される個人情報を管理する第１のサーバに、第１のネットワーク特定情報、第２のネットワーク特定情報、およびアクセス情報を含む制御情報が、サービス端末に供給され、サービス端末で、第２のネットワーク特定情報が保持され、自分自身に対するアクセスから、アクセス情報が取得され、取得されるように、第２のネットワーク特定情報およびアクセス情報が、携帯端末に供給され、供給された制御情報が、第１のサーバに供給され、第１のサーバで、第１のネットワーク特定情報により特定される個人情報が管理され、供給された制御情報に含まれる第２のネットワーク特定情報により特定される処理を実行する第２のサーバに、制御情報、個人情報、およびアクセス情報に基づくサービスの提供が要求され、第２のサーバで、第２のネットワーク特定情報により特定される処理が管理され、要求に基づいて、第２のネットワーク特定情報により特定される処理が、制御情報、個人情報、およびアクセス情報に基づいて実行される。

【００６３】

【発明の実施の形態】

図１は、本発明を適用したサービス提供システムの利用例を示している。この場合、ユーザＡは、サービス提供システムを利用して、料金の精算を行う。

【００６４】

腕時計１は、ユーザＡに身に着けられている腕時計であるが、この腕時計１には、携帯端末２と通信し、携帯端末２からの要求に応じて、一回の処理に限りパスワードとして利用される文字列等（以下、ワンタイムパスワードと称する）を、所定のアルゴリズムで発生し、携帯端末２に送信する機能を有するＩＣチップ（以下、認証データ用ＩＣチップと称する）（図２）が組み込まれている。

【００６５】

なお、腕時計１の他、指輪などに認証データ用ＩＣチップを組み込ませておくこともできる。すなわち、このように、身に着けておくことができる物に、認証

データ用ＩＣチップを組み込ませておくことで、このシステムの利用がより容易になる。

【００６６】

また、腕時計１に防水性を持たせ、いつでも（例えば、お風呂に入っているときにでも）身に着けておくことができるようにすることもできる。

【００６７】

携帯端末２は、携帯に便利な小型の装置で、ユーザＡによる操作に応じて、精算装置３－１を介してネットワーク４に接続し、例えば、個人サーバ５と通信する。携帯端末２は、個人サーバ５に記憶されているユーザＡの個人情報を指定するＵＲＬ（以下、ＵＲＬ１と称する）を記憶しており、そのＵＲＬ１を、精算装置３－１に送信し、精算装置３－１が、それに基づく通信を行うことで、個人サーバ５との通信が可能となる。

【００６８】

なお、ここでＵＲＬは、インターネット上のホームページの他、テキストデータ、処理プログラムなどを含む、ネットワーク４上に存在する資源を特定するができるものを意味する。

【００６９】

精算装置３－１は、ユーザ（この例の場合、ユーザＡ）が購入する商品の合計値を算出する装置、いわゆるレジであるが、この例の場合、無線で携帯端末２と通信することができるとともに、ネットワーク４を介して、個人サーバ５やサービスサーバ６－１とも通信することができる。すなわち、精算装置３－１は、携帯端末２に対するネットワークアクセスポートとしての役割を果たす。なお、明細書中の各図において、携帯端末２に対するネットワークアクセスポートの役割を有する装置には、ＮＡＰ（ネットワークアクセスポートの略）が付されている。

【００７０】

個人サーバ５は、ＵＲＬ１により特定される、ユーザＡの個人データを管理するサーバであり、ネットワーク４を介して、精算装置３－１やサービスサーバ６－１と通信する。

【００７１】

サービスサーバ６－１は、所定のＵＲＬ（以下、ＵＲＬ２と称する）により特定される処理をサーバである。サービスサーバ６－１が、その処理を、ネットワーク４を介して、精算装置３－１や個人サーバ５と通信して実行する。これにより、ユーザＡは、各種サービスの提供を受けることができる。

【００７２】

図２は、腕時計１に組み込まれた認証データ用ＩＣチップの構成例を示している。ＣＰＵ１１は、システムバス１３を介して接続されるメインメモリ１２に記憶されているプログラム（例えば、ワンタイムパスワード生成プログラム）を実行し、ワンタイムパスワード等を生成する。

【００７３】

通信部１４は、無線で携帯端末２と通信し、例えば、携帯端末２からの認証データ発生要求を受信して、ＣＰＵ１１に供給したり、ＣＰＵ１１により生成されたワンタイムパスワード等を、携帯端末２に送信する。

【００７４】

なお、通信部１４は、人体を媒体として携帯端末２と通信することができるようにすることができる。この場合、例えば、携帯端末２がユーザＡの手で直接保持されると、ユーザＡの体を媒体として、腕時計１（認証データ用ＩＣチップ）と携帯端末２の通信が可能となる。

【００７５】

電源供給部１５は、各部に電源を供給する。なお、電源供給部１５を、小型の電池の他、太陽電池で構成し、太陽光から光電変換で電源電力を得るようにすることもできる。また、電源供給部１５は、電磁誘導起電力、また人体からの熱による熱起電力を、電源電力とすることもできる。

【００７６】

図３は、携帯端末２の構成例を示している。ＣＰＵ２１は、メインメモリ２２に記憶されているプログラムに従って、各種の処理を実行する。

【００７７】

メインメモリ２２は、各種プログラムを記憶しているとともに、ＵＲＬ１（ユ

ーザＡの個人情報を特定するもの）を記憶している。なお、メインメモリ１２は、携帯端末２の電源が切られてもその記憶が保持されるＳＲＡＭで構成され、いわゆるバッテリーバックアップされている。また、メインメモリ２２は、高速動作可能なＳＲＡＭと、記憶保持用のフラッシュメモリ等の組み合わせで構成することもできる。

【００７８】

入力部２３は、ＣＰＵ２１に所定の指令を入力するときユーザにより適宜操作される。表示部２４は、例えば、ＬＣＤ等により構成され、所定の文字、図形、または画像を表示する。出力部２５は、スピーカ等で構成され、音声信号を出力する。

【００７９】

通信部２６は、赤外線通信や、ブルートゥースなどのようにミリ波帯、１３．５ＭＨz、または２０ＭＨz等の電波を利用して、精算装置３－１（ネットワークアクセスポート）と通信する。すなわち、携帯端末２と精算装置３－１の間では、いわゆる短距離通信が行われるので、ここでの通信により、例えば、心臓ペースメーカ等の精密装置が誤動作するようなことはない。従って、携帯端末２と精算装置３－１の通信を、場所の制限を受けずに行うことができる（場所の制限を受けずに、このシステムを利用することができる）。

【００８０】

通信部２７は、腕時計１に組み込まれている認証データ用ＩＣチップ（通信部１４）と無線で通信する。なお、通信部２７は、人体を媒体として認証データ用ＩＣチップと通信することもできる。

【００８１】

インターフェース２８は、入力部２３乃至通信部２７とＣＰＵ２１との間に配置され、インタフェース処理を行う。

【００８２】

図４は、精算装置３－１の構成例を示している。ＣＰＵ３１は、ＲＯＭ３２に記憶されているプログラムに従って、各種の処理を実行する。ＲＡＭ３３には、ＣＰＵ３１が各種の処理を実行する上において必要なデータなどが適宜記憶され

る。

【００８３】

入力部３４は、ＣＰＵ３１に所定の指令を入力するとき適宜操作される。表示部３５は、例えば、ＬＣＤ等により構成され、所定の文字、図形、または画像を表示する。ハードディスク３６は、所定のデータ（例えば、ＵＲＬ２）を記憶し、必要に応じて、これを再生する。

【００８４】

通信部３７は、ネットワーク４に接続されており、それを介して、個人サーバ５やサービスサーバ６－１と通信する。

【００８５】

通信部３８は、赤外線通信や、ブルートゥースなどのようにミリ波帯、１３．５ＭＨz、または２０ＭＨzの電波を利用して、携帯端末２と通信する。

【００８６】

インターフェース３９は、入力部３４乃至通信部３８とＣＰＵ３１との間に配置され、インタフェース処理を行う。

【００８７】

図５は、個人サーバ５の構成例を示してる。ＣＰＵ４１は、ＲＯＭ４２に記憶されているプログラムに従って、各種の処理を実行する。ＲＡＭ４３には、ＣＰＵ４１が各種の処理を実行する上において必要なデータなどが適宜記憶される。

【００８８】

なお、ＲＯＭ４２には、腕時計１（認証データ用ＩＣチップのメインメモリ１２）に記憶されているワンタイムパスワード等を生成するプログラムと同様のアルゴリズムでワンタイムパスワード等を生成するプログラムが記憶されている。すなわち、ＣＰＵ４１は、通信部４７、ネットワーク４、精算装置３－１、および携帯端末２を介して、腕時計１からのワンタイムパスワード等を受信した場合、そのプログラムを実行し、自分自身でもワンタイムパスワード等を生成する。そしてＣＰＵ４１は、受信したワンタイムパスワード等と生成したワンタイムパスワード等を照合して、ユーザ認証を行う。

【００８９】

入力部４４は、ＣＰＵ４１に所定の指令を入力するとき適宜操作される。表示部４５は、例えば、ＬＣＤ等により構成され、所定の文字、図形、または画像を表示する。

【００９０】

ハードディスク４６は、所定のデータ（例えば、このサービス提供システムに登録された正規のユーザ（ユーザＡなど）の氏名、住所、取引銀行の口座番号、ユーザの顔部分の画像データ（以下、顔写真データと称する）などの個人情報）を記憶し、これを、必要に応じて再生する。

【００９１】

通信部４７は、ネットワーク４に接続されており、ネットワーク４を介して、精算装置３－１やサービスサーバ６－１と通信する。

【００９２】

インターフェース４８は、入力部４４乃至通信部４７とＣＰＵ４１との間に配置され、インタフェース処理を行う。

【００９３】

サービスサーバ６－１の構成は、基本的に個人サーバ５の場合と同様であるので、その図示および説明は省略するが、そのＲＯＭまたはハードディスクには、ＵＲＬ２で特定される処理を実行するためのプログラムが格納されている。

【００９４】

次に、精算処理の手順を、図６のフローチャートを参照して説明する。

【００９５】

ステップＳ１において、精算装置３－１は、ＵＲＬ２、金額を示す情報（以下、購入金額と称する）、および支払ＩＤを、携帯端末２に送信する。携帯端末２は、それを受信する。

【００９６】

このとき、ユーザＡは、購入する商品を、精算装置３－１の付近に設けられた台に運ぶ。店員は、ユーザＡにより運ばれた商品の購入金額（合計金額）を、精算装置３－１の入力部３４を操作して、算出した後、所定の操作を、精算装置３－１に対して行う。これにより、精算装置３－１は、その操作に対応して、上述

したようなデータを、携帯端末２に送信する。なお、このとき、ユーザＡ（携帯端末２）は、携帯端末２と精算装置３－１との短距離通信が可能となる程度に、精算装置３－１に近づいている。

【００９７】

次に、ステップＳ２において、携帯端末２は、ステップＳ１で受信したＵＲＬ２、購入金額、および支払ＩＤを、精算装置３－１およびネットワーク４を介して、個人サーバ５に送信するとともに、ＵＲＬ２により特定される処理を実行するサービスサーバ６－１との通信を、個人サーバ５に対して要求する。なお、携帯端末２と個人サーバ５との通信は、携帯端末２が、ＵＲＬ１を、精算装置３－１に送信し、精算装置３－１が、それに基づく通信を行うことで可能となる。これにより、個人サーバ５は、携帯端末２から送信されたデータを受信するとともに、その要求を認識する。

【００９８】

例えば、このとき、携帯端末２のＣＰＵ２１は、表示部２４を制御して、ステップＳ１で受信した情報を表示させる。ユーザＡは、表示部２４に表示された情報を確認すると、入力部２３に対して所定の操作を行う。これにより、携帯端末２は、その操作に対応して、ステップＳ１で受信した情報を、個人サーバ５に送信する。

【００９９】

ステップＳ３において、個人サーバ５は、ステップＳ２で認識した要求に基づいて、サービスサーバ６－１に対して、接続を要求する。サービスサーバ６－１は、その要求に応答する。これにより、個人サーバ５とサービスサーバ６－１との通信が確立される。

【０１００】

次に、ステップＳ４において、個人サーバ５は、ステップＳ２で受信した支払ＩＤと購入金額を、サービスサーバ６－１に送信し、サービスサーバ６－１は、それを受信する。

【０１０１】

ステップＳ５において、サービスサーバ６－１は、個人サーバ５に対して、ユ

ーザ認証を要求する。個人サーバ５は、その要求を認識する。

【０１０２】

次に、ステップＳ６において、顔写真データによるユーザ認証処理が行われる。ここでの処理の詳細は、図７のフローチャートに示されている。

【０１０３】

ステップＳ２１において、個人サーバ５は、ユーザＡの個人情報として記憶している顔写真データを、精算装置３－１に送信する。精算装置３－１は、それを受信する。次に、ステップＳ２２において、精算装置３－１は、顔写真データに対応する画像を表示部３５に表示する。

【０１０４】

ステップＳ２３において、精算装置３－１は、顔写真によるユーザ認証結果を認識する。具体的には、店員は、精算装置３－１の表示部３５に表示された顔の画像から、ユーザＡ本人であるか否かを確認する、すなわち、このシステムに正規に登録されたユーザであるか否かを確認する。そして店員は、その確認結果に応じた操作を、精算装置３－１の入力部３４に対して行う。これにより、精算装置３－１は、顔写真によるユーザ認証結果を認識する。

【０１０５】

次に、ステップＳ２４において、精算装置３－１は、ステップＳ２３で認識したユーザ認証結果を、個人サーバ５とサービスサーバ６－１に送信する。個人サーバ５とサービスサーバ６－１は、それを受信する。なお、ここでは、ユーザＡは、正規のユーザであると認証されたものとして、以下の説明を進める。

【０１０６】

その後、処理は終了し、図６のステップＳ７に進む。

【０１０７】

ステップＳ６で、精算装置３－１から供給された認証結果が、ユーザＡが、このシステムの正規のユーザである旨を示しているとき、ステップＳ７において、認証データによるユーザ認証が行われる。ここでの処理は、図８のフローチャートに示されている。

【０１０８】

ステップＳ３１において、個人サーバ５は、認証データの提供を、ネットワーク４および精算装置３－１を介して、携帯端末２に要求する。携帯端末２は、その要求を認識する。なお、個人サーバ５と携帯端末２との通信は、常に、ネットワーク４および精算装置３－１を介して行われるので、以下において、個人サーバ５と携帯端末２の通信について記述する場合、「ネットワーク４および精算装置３－１を介して」の文言を、適宜省略する。

【０１０９】

次に、ステップＳ３２において、携帯端末２は、ステップＳ３１で認識した要求に基づいて、認証データとしてのワンタイムパスワードを、腕時計１から取得する。具体的には、携帯端末２のＣＰＵ２１は、はじめに、表示部２４を制御して、認証データの提供が要求されていることを示すメッセージを表示させる。これにより、ユーザＡは、腕時計１を携帯端末２に近づける。（または携帯端末２を手で直接保持する）。その結果、腕時計１（認証データ用ＩＣチップ）と携帯端末２との通信が可能となるので、携帯端末２は、認証データの発生を、認識データ用ＩＣチップに対し要求し、認証データ用ＩＣチップは、その要求に応じてワンタイムパスワードを発生し、携帯端末２に送信する。携帯端末２は、腕時計１からのワンタイムパスワードを受信する。このようにして、携帯端末２は、認証データとしてのワンタイムパスワードを取得する。

【０１１０】

ステップＳ３３において、携帯端末２は、ステップＳ３２で取得した認証データを、個人サーバ５に送信する。個人サーバ５は、それを受信する。

【０１１１】

次に、ステップＳ３４において、個人サーバ５は、自分自身でワンタイムパスワードを生成して、ステップＳ３３で受信した認証データと照合し、ユーザ認証を行う。具体的には、上述したように、個人サーバ５のＣＰＵ４１は、ＲＯＭ４２に記憶されている、認証データ用ＩＣチップが実行するワンタイムパスワード生成プログラムと同様のアルゴリズムでワンタイムパスワードを生成して、受信したワンタイムパスワードと照合する。両者が同じであれば、正規のユーザであると認証される。

【０１１２】

ステップＳ３５において、個人サーバ５は、ユーザ認証の結果を、サービスサーバ６－１に送信する。サービスサーバ６－１は、それを受信する。

【０１１３】

なお、ここで、ユーザ認証が成立した場合（この例の場合、ユーザＡが正規のユーザであると認証された場合）、個人サーバ５は、ワンタイムパスワードの生成アルゴリズムの更新を行うとともに、その更新に関する情報を、携帯端末２を介して、腕時計１（認証データ用ＩＣチップ）にも送信する。認証データ用ＩＣチップは、それを受信する。これにより、認証データ用ＩＣチップは、個人サーバ５が行った更新に対応させて、自分自身のワンタイムパスワードの生成アルゴリズムを更新する。

【０１１４】

このように、ユーザ認証が成立したとき、認証データ発生ＩＣチップと個人サーバ５（認証される側と認証する側）のワンタイムパスワードの生成アルゴリズムを更新することで、本システムの不正利用を防止することができる。例えば、ワンタイムパスワードのアルゴリズムが更新されているので、認証データ発生ＩＣチップ自体が複製されても、それが発生するワンタイムパスワードでは、ユーザの認証を得ることができない。

【０１１５】

その後、処理は終了し、図６のステップＳ８に進む。なお、ここでは、認証データによるユーザ認証により、ユーザＡが正規のユーザであると認証されたものとして、以下の説明を進める。

【０１１６】

ユーザＡが、正規のユーザであると認証されると、ステップＳ８において、支払処理が行われる。具体的には、サービスサーバ６－１は、料金の振り込み先を、個人サーバ５に通知する。

【０１１７】

個人サーバ５は、通知された振り込み先のサーバＡ（図示せず）に対して、所定の振り込み処理を行い、振り込みが完了すると、その旨を、サービスサーバ６

－１に送信する。なお、このとき個人サーバ５は、例えば、支払ＩＤを添付して電子マネー等をサーバＡに送信し、サーバＡでは、その支払ＩＤを利用して、決済することもできる。なお、ここでは、購入金額に対する支払が完了したものとして、以下の説明を進める。

【０１１８】

購入金額に対する支払が完了すると、ステップＳ９において、サービスサーバ６－１は、ステップＳ４で受信した支払ＩＤを、精算装置３－１に送信する（戻す）。精算装置３－１は、それを受信する。

【０１１９】

ステップＳ１０において、精算装置３－１は、支払処理の完了を認識する。具体的には、精算装置３－１のＣＰＵ３１は、表示部３５を制御して、ステップＳ９で受信した支払ＩＤを表示させる。これにより、店員は、購入金額に対する支払が完了したことを確認し、所定の操作を精算装置３－１の入力部３４に対して行う。これにより、精算装置３－１は、支払処理の完了を認識する。

【０１２０】

その後、処理は終了する。このようにして、購入金額に対する精算が行われる。

【０１２１】

このように、ユーザＡの個人情報は、個人サーバ５に記憶され、携帯端末２には記憶されていないので、例えば、携帯端末２を紛失しても、個人情報が第３者に渡り、悪用されることがない。

【０１２２】

また、携帯端末２とネットワークアクセスポート（精算装置３）との通信は、いわゆる短距離通信であり、心臓ペースメーカ等の精密機器の動作に影響を与えないので、ユーザは、いつでも、携帯端末２で精算装置３と通信を行い、このシステムを利用することができる。

【０１２３】

なお、以上においては、ネットワークアクセスポートとしての精算装置３が設けられている場合を例としてが、携帯端末２が個人サーバ５等と直接通信するこ

とができるようにすることもできる。

【０１２４】

また、以上においては、ステップＳ６での顔写真によるユーザ認証、およびステップＳ７での認証データによるユーザ認証のそれぞれを行うようにしたが、例えば、いずれか一方のユーザ認証だけを行うようにすることもできる。

【０１２５】

また、以上においては、認証データとして、腕時計１が発生するワンタイムパスワードを利用する場合を例として説明したが、携帯端末２と個人サーバ５との共通鍵で暗号化されたパスワード、または個人サーバ５の公開鍵で暗号化されたパスワードを認証データとすることもできる。さらに、認証データとして、ユーザの指紋、声紋、虹彩、または特定部分の血管の造影等を利用することができる。また、携帯端末２は、個人サーバ５からの要求に応じて、認証用ＩＣチップから適切な応答があったとき、認証用ＩＣチップから、認証データを取得するようにすることができる。

【０１２６】

図９は、指紋および声紋を認証データとして採取することができる携帯端末２の構成例を示している。すなわち、この携帯端末２には、図３の携帯端末２に、指紋を採取するための指紋採取センサ５１と、音声を取り込むマイクロフォン５２がさらに設けられている。

【０１２７】

指紋採取センサー５１は、ユーザＡが指先の内側（腹）を押し当てることができるように取り付けられており、指の腹が押し当てられたとき、その指紋データを採取し、ＣＰＵ２１に出力する。またはマイクロフォン５２は、ユーザＡの音声を取り込みＣＰＵ２１に出力する。

【０１２８】

ＣＰＵ２１は、指紋採取センサ５１からの指紋データ、またはマイクロフォン５２からの音声データを解析し、その特徴データを認証データとして取得する。

【０１２９】

なお、認証データとしての指紋や声紋の特徴データは、その個人を特定するデ

ータとして重要であるので、指紋や声紋を認証データとして利用する場合、例えば、図８のステップＳ３３の処理で、認証データを、個人サーバ５に送信するとき、暗号化する必要がある。

【０１３０】

この場合、携帯端末２は、ＵＲＬ１の公開鍵を保持しており、取得した認証データ（指紋又は声紋等の特徴データ）を、そのＵＲＬ１の公開鍵とともに、精算装置３－１に送信する。精算装置３－１は、それらを受信する。なお、携帯端末２と精算装置３－１の通信は、短距離通信であるので、送信データが改竄される可能性は少ないことから、この例の場合、携帯端末２と精算装置３－１との通信では、認証データは、暗号化されない。ただし、携帯端末２が自身が暗号化することもできる。

【０１３１】

精算装置３－１は、受信したＵＲＬ１の公開鍵で、認証データを暗号化し、個人サーバ５に送信する。個人サーバ５は、それを受信する。

【０１３２】

個人サーバ５は、この場合、ＵＲＬ１の秘密鍵を保持しており、それを利用して、精算装置３－１からの認証データの暗号化を解凍する。

【０１３３】

個人サーバ５はまた、この場合、ユーザＡの指紋や声紋等の特徴データを認証データとして予め（ユーザＡの登録時に）記憶しており、図８のステップＳ３４の処理で、暗号化を解凍して得られた認証データと、記憶している認証データとを照合し、ユーザＡを認証する。

【０１３４】

このように、認証データの暗号化が必要な場合、ネットワークアクセスポートとしての精算装置３－１で暗号化するようにしたので、携帯端末２で暗号化を行う場合に比べ、より強固な暗号化を行うことができる。通常、携帯端末２は、小型である必要など、設計上の制限から、強固な暗号化を行うプログラムを実装することができない。

【０１３５】

また、図８のステップＳ３５で、ワンタイムパスワードの生成アルゴリズムを更新する際に、携帯端末２が保持するＵＲＬ１の公開鍵と、個人サーバ５が保持するＵＲＬ１の秘密鍵を、それぞれ対応させて変更することができる。このように、鍵自身を変更することで、より強固な暗号化が可能となる。

【０１３６】

また、個人サーバ５から、所定の情報を暗号化して、携帯端末２に送信したい場合、個人サーバ５は、携帯端末２の公開鍵を、ユーザＡの個人情報として保持し、その公開鍵で、情報を暗号化して、携帯端末２に送信する。携帯端末２は、自分の秘密鍵で、個人サーバ５からの情報の暗号化を解凍する。この場合、ユーザ認証結果に応じて、それぞれの鍵を変更することができる。

【０１３７】

また、図６の例における、ステップＳ８での支払処理は、銀行の口座に預けられているお金（現金）による支払を想定しているが、いわゆる商品券を利用する支払を行うこともできる。なお、ここでの商品券とは、それを利用することができる店舗の公開鍵で暗号化された、そこで購入することができる金額を示すデータ（商品券データ）を意味し、例えば、ユーザＡが持っている商品券は、個人サーバ５（ハードディスク４６）に、ユーザＡの個人情報として記憶されている。

【０１３８】

商品券を利用した精算処理の手順を、図１０のフローチャートを参照して説明する。

【０１３９】

ステップＳ４０乃至ステップＳ４６、およびステップＳ４８，Ｓ４９においては、図６のステップＳ１乃至ステップＳ７、およびステップＳ９，Ｓ１０の場合と同様の処理が行われるので、その説明は省略する。

【０１４０】

ステップＳ４７において、商品券による支払処理が行われる。ここでの処理の詳細は、図１１のフローチャートに示されている。

【０１４１】

ステップＳ５１において、個人サーバ５は、サービスサーバ６－１の公開鍵で

暗号化された商品券データを、サービスサーバ６－１に送信する。サービスサーバ６－１は、それを受信する。

【０１４２】

次に、ステップＳ５２において、サービスサーバ６－１は、自分の秘密鍵で、ステップＳ５１で受信した商品券データを解凍する。この場合、サービスサーバ６－１は、自分の秘密鍵および公開鍵を予め保持している。

【０１４３】

ステップＳ５３において、サービスサーバ６－１は、商品券データに示される購入可能金額から、ステップＳ４３で受信した購入金額を減算する。

【０１４４】

次に、ステップＳ５４において、サービスサーバ６－１は、その減算結果を、個人サーバ５の公開鍵で暗号化して、商品券データを生成（更新）し、個人サーバ５に送信する。個人サーバ５は、それを受信する。

【０１４５】

ステップＳ５５において、個人サーバ５は、ステップＳ５４で受信した商品券データを、ユーザＡの個人情報として記憶する。

【０１４６】

その後、処理は終了し、図９のステップＳ４８に進む。このようにして、商品券による支払が行われる。

【０１４７】

また、図６の例では、ユーザＡが購入する商品を、精算装置３－１（レジ）まで持っていき、そして精算装置３－１で算出された購入金額分の料金を支払う場合を例として説明したが、次に、例えば、大きくて、精算装置３まで運ぶことができない商品を購入する場合について説明する。

【０１４８】

図１２は、この場合に利用される携帯端末２の構成例が示されている。なお図中、図３における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。

【０１４９】

すなわち、この携帯端末２には、図３の携帯端末２に、イメージセンサ６１がさらに設けられている。

【０１５０】

イメージセンサ６１は、この例の場合商品に付されているＵＲＬ２（例えば、商品のタグに付されているＵＲＬ２）を、画像データとして取得するセンサーである。ＣＰＵ２１は、イメージセンサ６１により取得された画像データから、ＵＲＬ２を認識する。

【０１５１】

次に、この場合の精算処理の手順について、図１３のフローチャートを参照して説明する。なお、この場合、ＵＲＬ２が付された商品の近くにネットワークアクセスポート（図示せず）が設定されているものとする。

【０１５２】

ステップＳ６１において、携帯端末２（ＣＰＵ２１）は、イメージセンサ６１により得られた画像データから、商品に付されたＵＲＬ２を取得する。

【０１５３】

次に、ステップＳ６２において、携帯端末２は、ステップＳ６１で取得したＵＲＬ２および商品購入を示す信号を、図示せぬネットワークアクセスポートおよびネットワーク４を介して、個人サーバ５に送信するとともに、ＵＲＬ２を管理するサービスサーバ６－１との通信を要求する。

【０１５４】

なお、ステップＳ６１またはステップＳ６２での携帯端末２の動作は、ユーザＡによる携帯端末２に対する所定の動作に対応して行われる。また、このとき、ユーザＡ（携帯端末２）は、携帯端末２とネットワークアクセスポートとの短距離通信が可能となる程度に、ネットワークアクセスポートに近づいているものとする。

【０１５５】

ステップＳ６３において、個人サーバ５とサービスサーバ６－１の通信が確立されると、ステップＳ６４において、個人サーバ５は、ＵＲＬ２により指定される商品の購入を示す信号を、サービスサーバ６－１に送信する。サービスサーバ

６－１は、それを受信する。

【０１５６】

ステップＳ６５において、サービスサーバ６－１は、個人サーバ５に対して、ユーザ認証を要求する。個人サーバ５は、その要求を認識する。

【０１５７】

ステップＳ６６において、認証データによるユーザ認証が行われる。ここでの処理は、図６のステップＳ７での処理と同様にして行われるので、その説明は省略する。

【０１５８】

ステップＳ６６の処理で、ユーザＡが正規のユーザであると認証されると、ステップＳ６７において、サービスサーバ６－１は、ＵＲＬ２で示される商品の商品情報（例えば、価格情報や商品の紹介情報）を、個人サーバ５に送信する。個人サーバ５は、それを受信し、そして携帯端末２に送信する。携帯端末２は、それを受信する。

【０１５９】

ステップＳ６８において、携帯端末２は、商品が購入されるか否かを認識する。具体的には、携帯端末２のＣＰＵ２１は、ステップＳ６７で受信した商品情報を、表示部２４に表示させる。ユーザＡは、表示部２４に表示された商品情報に基づいて、その商品を購入するか否かを判断し、その判断結果に応じた操作を、入力部２３に対して行う。これにより、ＣＰＵ２１は、商品が購入されるか否かを認識する。

【０１６０】

ユーザＡにより、商品購入のための操作が携帯端末２の入力部２３に対して行われると、ステップＳ６９において、支払処理が行われる。ここでの処理は、図６のステップＳ８での処理と同様であるので、その説明は省略する。

【０１６１】

なお、例えば、オークション等のように、商品の価格が短い時間内で変動する場合、ステップＳ６７，６８での処理が繰り返し実行され、ユーザは、随時変化する商品価格を参考にして、その商品の購入を決定することができる。またこの

とき、ユーザＡは、携帯端末２の入力部２３を操作し、希望価格を入力して、そのオークションに参加することができる。

【０１６２】

また、図１３の例では、イメージセンサ６１により取得された画像データから、ＵＲＬ２を取得する場合を例として説明したが、商品に、ＵＲＬ２を示すバーコード（２次元バーコードを含む）が付されている場合、携帯端末２は、バーコードリーダを備え、それでＵＲＬ２を読み取ることができる。

【０１６３】

また、ＵＲＬ２が、例えば、その商品の宣伝用の音声に、間欠的に、聞こえない帯域に含まれている場合、携帯端末２は、マイクロフォン５２（図９）で、その音声を取り込み、ＵＲＬ２を抽出するようにすることもできる。さらに、ＵＲＬ２が、赤外線で出力されている場合、携帯端末２は、赤外線センサを備え、その赤外線センサにより受光された赤外線から、ＵＲＬ２を抽出したり、ＵＲＬ２が、高周波で所定の送信装置から出力されている場合、携帯端末２は、高周波アンテナを備え、高周波アンテナにより受信された高周波から、ＵＲＬ２を抽出する。

【０１６４】

また、図１３の例では、商品情報が携帯端末２の表示部２４に表示される場合を例として説明したが、より大きな画面で表示した方がよい場合等では、図１４に示すように、その商品の近くに設けられている、ネットワークアクセスポートとしてのモニタ３－２に、それを表示させることができる。なお、本明細書においては、携帯端末２に対するネットワークアクセスポートとしての機能を有する装置には、”３－”の符号を付してあり、その構成は、精算装置３－１の構成（図４）と基本的に同様である。

【０１６５】

この場合、基本的には、図１３のフローチャートの場合と同様の処理が行われるが、ステップＳ６２に相当する処理で、携帯端末２は、個人サーバ５に、ＵＲＬ２および商品購入を示す信号とともに、モニタ３－２のＵＲＬ（ＵＲＬ３）を送信する。すなわち、この処理に先立って、ユーザは、見えるように示されてい

る（例えば、モニタ３－２に付されている）モニタ３－２のＵＲＬ３を確認し、それを、携帯端末２の入力部２３に入力する。

【０１６６】

これにより、ステップＳ６７に相当する処理で、サービスサーバ６－１は、商品情報等を、モニタ３－２に送信する。モニタ３－２は、それを受信し、表示する。

【０１６７】

また、このような利用によれば、例えば、サービスサーバ６－１が、コンテンツ（楽曲または映像のデータ）を配信する場合、ユーザＡは、コンテンツを購入し、それを自分自身の再生装置（例えば、オーディオ装置やモニタ）に送信させることで、それを見たり聞いたりすることができる。また、再生装置ではなく、個人サーバ５に送信させて、そこに記憶させておくことで、ユーザＡは、後からそれを利用することができる。

【０１６８】

また、サービスサーバ６－１が、コンテンツとして楽曲データを提供する場合、１つの宣伝方法として、この楽曲を流すとき（例えば、店内放送や、ラジオ放送で流すとき）、その中にそのコンテンツのＵＲＬ２を含ませておけば、ユーザＡは、それを聴いて気に入れば、携帯端末２を操作し、マイクロフォン（マイクロファン５２）からその楽曲を読み取り、ＵＲＬ２を取得することで、そのコンテンツを、再生装置や個人サーバ５に供給させることができる。

【０１６９】

また、図１３の例では、サービスサーバ６－１が保持している商品情報をモニタ３－２に表示させる場合を例として説明したが、モニタ３－２がその情報を保持しているようにすることもできる。

【０１７０】

また、図１３の例では、１つの商品のＵＲＬ２を取得し、それについての支払処理を説明したが、ユーザＡは、興味のある複数の商品（実際購入するかはこの時点ではわからない商品）のＵＲＬ２（商品によってそれぞれ異なるＵＲＬ）を取得して、随時その商品情報の提供を受け、後から、その商品情報を参照して、

最終的に購入する商品を決定することもできる。

【０１７１】

この場合、提供を受けた商品情報を、個人サーバ５が記憶（キャッシュ）し、携帯端末２から要求があった場合、個人サーバ５は、要求された商品情報を、携帯端末２に送信するようにする。このようにすることで、個人サーバ５が記憶している情報について、サービスサーバ６－１に再度アクセスする必要がなくなるので、必要な情報を迅速に閲覧することができ、また通信コスト等を節約することができる。また、例えば、携帯端末２が、個人サーバ５を介して、サービスサーバ６－１に対するウエブブラウジング等を行い、所定のページを閲覧した場合、個人サーバ５が、このときの操作情報をキャッシュしておき、それを、再度そのページを閲覧する際に利用するようにできる。これにより、迅速にそのページにたどり着くことができる。

【０１７２】

なお、個人サーバ５の他、携帯端末２もデータをキャッシュすることもできる。しかしながら、この場合、個人情報がキャッシュされると、携帯端末２を紛失したとき、その情報が第３者に漏洩することもあり得るので、個人サーバ５は、個人情報を、携帯端末２に送信する際に、その個人情報に、そのキャッシュを許可しない旨を示すタグを付して送信する。このようにすることで、個人サーバ５から送信された個人情報は、携帯端末２でキャッシュされず、携帯端末２が例えば紛失しても、個人情報が、第３者に渡ることを防止することができる。

【０１７３】

また、個人サーバ５が記憶する情報量には制限があり、その制限を超える場合、記憶している情報を消去する必要がある。このとき、個人サーバ５は、ブックマーク等に登録されていないもの、またはブックマーク等に登録されたページからのリンクに成っていないデータから優先的に消去する。またさらに情報の消去が必要な場合、個人サーバ５は、ブックマークの中で優先順位を設け、その低いものから消去する。

【０１７４】

図１５は、本発明を適用したサービス提供システムの他の利用例を示している

。この場合、ユーザＡは、ブラウジング装置および携帯端末２のネットワークアクセスポートとしてのパーソナルコンピュータ３－３を利用して、ショッピングサーバ６－２に対するネットショッピングを行う。なお、本明細書においては、サービスを提供するサーバには、”６－”の符号を付してあり、その構成は、個人サーバ５の構成（図５）と基本的に同様である。

【０１７５】

ネットショッピングを行う場合の処理手順は、図１６のフローチャートに示されている。

【０１７６】

ステップＳ８１において、パーソナルコンピュータ３－３は、ネットワーク４を介して、ショッピングサーバ６－２にアクセスする。ステップＳ８２において、パーソナルコンピュータ３－３は、購入される商品を認識し、ステップＳ８３において、そのＵＲＬ（ＵＲＬ２）を、携帯端末２に送信する。携帯端末２は、それを受信する。なお、このとき、ユーザＡ（携帯端末２）は、携帯端末２とパーソナルコンピュータ３－３との短距離通信が可能となる程度に、パーソナルコンピュータ３－３に近づいているものとする。

【０１７７】

ステップＳ８１乃至ステップＳ８３でのパーソナルコンピュータ３－３の動作は、ユーザＡによる、パーソナルコンピュータ３－３の、例えば、キーボード等に対する操作に基づいて実行される。

【０１７８】

次に、ステップＳ８４において、携帯端末２は、個人サーバ５に、ステップＳ８３で受信したＵＲＬ２を、パーソナルコンピュータ３－３およびネットワーク４を介して送信するとともに、ＵＲＬ２を管理するショッピングサーバ６－２との通信を要求する。個人サーバ５は、ＵＲＬ２を受信するとともに、その要求を認識する。

【０１７９】

ステップＳ８５で、個人サーバ５とショッピングサーバ６－２との通信が確立されると、ステップＳ８６において、個人サーバ５は、ＵＲＬ２を、ショッピン

グサーバ６－２に送信し、ショッピングサーバ６－２は、それを受信する。

【０１８０】

次に、ステップＳ８７において、ショッピングサーバ６－２は、個人サーバ５に対して、ユーザ認証を要求する。個人サーバ５は、その要求の認識する。

【０１８１】

ステップＳ８８において、認証データによるユーザ認証が行われるが、ここでの処理は、図６のステップＳ７における処理と同様であるので、その説明は省略する。

【０１８２】

ステップＳ８８で、ユーザＡが、正規のユーザであると認証されると、ステップＳ８９において、支払処理が行われる。ここでの処理は、基本的には、図６のステップＳ８における処理と同様であるが、ＵＲＬ２で示される商品の金額情報等が、ショッピングサーバ６－２から個人サーバ５に送信され、個人サーバ５は、その額に応じた振り込み処理を行う。

【０１８３】

ステップＳ８９で、支払処理が完了すると（支払が成立すると）、ステップＳ９０において、商品発送のための処理が行われる。具体的には、ショッピングサーバ６－２は、例えば、ユーザＡの住所を、配送先として、個人サーバ５から取得し、配送を管理する他のサーバ（図示せず）（以下、配送サーバと称する）に送信する。配送業者は、配送サーバから得られた配送先に、ユーザＡにより購入された商品を配送する。

【０１８４】

ステップＳ９１において、ショッピングサーバ６－２は、配送処理の内容を、パーソナルコンピュータ３－３に送信する。パーソナルコンピュータ３－３は、それを受信し、表示する。これにより、ユーザＡは、配送手続きが完了したことを（例えば、配送先が決定したことを）、を確認することができる。

【０１８５】

なお、配送サーバは、個人サーバ５に、配送の状況（例えば、商品の出荷日、現在保管されている配送センター）を、例えば、定期的に提供するようになされ

ているので、ユーザＡは、携帯端末２を介して、その情報を参照することができる。

【０１８６】

また、配送先が、個人サーバ５に個人情報として記憶されてない場合、ユーザＡは、携帯端末２を操作して、希望する配信先を、ショッピングサーバ６－２に通知することができる。また、配信先を、例えば、ユーザＡの住所で指定する他、「住所から最も近い、コンビニエンスストアー」など、抽象的に指定することもできる。この場合、ショッピングサーバ６－２は、個人サーバ５から取得したユーザＡの住所から最も近いコンビニエンスストアーを探し出し、そこを配送先として、配送サーバに通知する。

【０１８７】

また、図１６（図１５）の例では、パーソナルコンピュータ３－３を介してネットショッピングを行ったが、このパーソナルコンピュータ３－３は、ユーザＡが所有するものに限られない。例えば、このサービス提供システムの業者が、パーソナルコンピュータ３－３（ネットワークアクセスポート）を、例えば、レストラン、または街頭に配置すれば、ユーザＡは、それを利用して、上述したようなサービスの提供を受けることができる。

【０１８８】

しかしながら、この場合、ネットワークアクセスポートを利用したユーザＡに、このときの、サービス提供システムの使用料等を請求する必要がある。図１７には、サービス提供システムの使用料を管理するネットワークアクセスポート管理サーバ（以下、管理サーバと略称する）７１が図示されている。管理サーバ７１は、ネットワーク４を介してネットワークアクセスポート３と個人サーバ５と通信して、ＵＲＬ４により特定される、使用料の精算処理を実行する。

【０１８９】

次に、サービス提供システムの使用料に対する精算処理の手順を、図１８のフローチャートを参照して説明する。

【０１９０】

ステップＳ１０１において、ネットワークアクセスポート３は、一連のトラン

ザクションで転送したデータの量（例えば、携帯端末２または個人サーバ５に転送したデータ量）を算出する。

【０１９１】

次に、ステップＳ１０２において、ネットワークアクセスポート３は、個人サーバ５に、ステップＳ１０１で算出したデータ転送量、ＵＲＬ４、および自分自身の位置を示す情報（位置情報）を送信するとともに、ＵＲＬ４により特定される処理を実行する管理サーバ７１との通信を要求する。個人サーバ５は、それらのデータを受信するとともに、その要求を認識する。なお、個人サーバ５は、受信した位置情報を、ユーザＡの個人情報として記憶する。また、ネットワークアクセスポート３は、ＵＲＬ４を保持している。

【０１９２】

ステップＳ１０３において、個人サーバ５と管理サーバ７１との通信が確立されると、ステップＳ１０４において、個人サーバ５は、ステップＳ１０２で受信した、位置情報、ＵＲＬ４、およびデータ転送量を、管理サーバ７１に送信する。管理サーバ７１は、それらを受信する。

【０１９３】

次に、ステップＳ１０５において、管理サーバ７１は、ユーザ認証を、個人サーバ５に対して要求する。ステップＳ１０６において、個人サーバ５は、認証データによるユーザ認証を行う。ここでの処理は、図６のステップＳ７における処理と同様であるので、その説明は省略する。

【０１９４】

ステップＳ１０６で、ユーザＡが、正規のユーザであると認証されると、ステップＳ１０７において、管理サーバ７１は、ステップＳ１０４で受信した位置情報に基づいて、ネットワークアクセスポート３が不正利用されているか否かを判定する。

【０１９５】

例えば、ユーザＡの契約において、利用地域が制限されている場合、その位置情報が、契約地域外の地域を示している場合、不正利用（契約外の利用）と判定される。また、アクセス間隔（時間）から見て、到底移動できない距離だけ離れ

ているネットワークアクセスポートのそれぞれを介して、アクセスがあった場合、不正利用されていると判定される。

【０１９６】

ステップＳ１０７で、不正利用されていないと判定された場合、ステップＳ１０８に進み、支払処理が行われる。具体的には、管理サーバ７１は、ＵＲＬ４により特定される決済処理を実行する。これにより、ステップＳ１０１で算出されたデータ転送量に応じた、システムの使用料金の支払が行われる。

【０１９７】

ステップＳ１０７で、不正利用されていると判定された場合、ステップＳ１０９に進み、所定の処理が実行される。

【０１９８】

ステップＳ１０８またはステップＳ１０９の後、処理は終了する。なお、ここでは、管理サーバ７１が、ネットワークアクセスポート３の位置情報に基づいて、ネットワークアクセスポート３の不正利用を判定する場合を例として説明したが、上述した、例えば、サービスサーバ６－１が、精算装置３－１の位置情報を取得し、精算装置３－１が不正利用されているか否かを判定することもできる。

【０１９９】

また、図１，１４，１５，１７の例では、一人のユーザＡによる利用について説明したが、実際は、図１９に示すように、他のユーザ（ユーザＢ）も、他の携帯端末Ｂで、このシステムを利用する。すなわち、個人サーバ５は、多くのユーザの個人情報を、それぞれのＵＲＬ１に基づいて管理している。

【０２００】

ここで、個人サーバ５において、ユーザＡの個人情報として管理されている、ユーザＡが購入したコンテンツを、ユーザＢが利用する場合の処理手順を説明する。

【０２０１】

携帯端末２または携帯端末Ｂから、ユーザＡが購入した所定のコンテンツを、ユーザＢが使用する旨が通知されると、個人サーバ５は、そのコンテンツを記憶している場所（アドレス）を、携帯端末Ｂに送信する。携帯端末Ｂは、それを受

信し、記憶する。ユーザＢは、コンテンツを利用したいとき、携帯端末Ｂを操作して、先に記憶したアドレスに従って、コンテンツを取得する。

【０２０２】

このようにすることで、個人サーバ５は、コンテンツを重複して保持する必要がない（同一のコンテンツを、ユーザＡおよびユーザＢの個人情報として保持する必要がない）。また、ユーザＢが実際にコンテンツを利用するまでは、携帯端末Ｂは、それを保持する必要がない。すなわち、個人サーバ５または携帯端末Ｂは、コンテンツを効率よく保持することができる。

【０２０３】

なお、購入されたコンテンツなどは、上述したように、ネットワーク４を介して転送され得るので、転送可能な情報として個人サーバ５に記憶されるが、ユーザの、住所、電話番号等の情報は、通常転送されないので、転送できない情報として個人サーバ５に記憶されるようになされている。

【０２０４】

図２０は、本発明を適用したサービス提供システムの他の利用例を示している。この場合、サービス提供システムにより電車の改札処理が行われる。

【０２０５】

改札機３－４は、ユーザＡが入札する駅Ａの改札口に設置されている改札機であり、改札機３－５は、ユーザＡが出札する駅Ｂの改札口に設置されている改札機である。改札機３－４，３－５は共に、ネットワークアクセスポートとしての機能を有し、駅サーバ６－３および駅サーバ６－４と通信する。

【０２０６】

駅サーバ６－３は、ＵＲＬ２－１により特定される、駅Ａの改札機３－４での入札に関する情報を管理する処理を実行し、駅サーバ６－４は、ＵＲＬ２－２により特定される、駅Ｂの改札機３－５での出札に関する情報を管理する処理を実行する。

【０２０７】

次に、入札処理の手順を、図２１のフローチャートを参照して説明する。

【０２０８】

ステップＳ１１１において、駅Ａの改札機３－４は、ＵＲＬ２－１、入札時刻、および駅ＡのＩＤを、携帯端末２に送信する。携帯端末２は、それらを受信する。このとき、ユーザＡ（携帯端末２）は、携帯端末２と改札機３－４との短距離通信が可能となる程度に、改札機３－４に近づいているものとする。

【０２０９】

次に、ステップＳ１１２において、携帯端末２は、個人サーバ５に、ステップＳ１１１で受信したＵＲＬ２－１、入札時刻、および駅ＡのＩＤを、改札機３－４およびネットワーク４を介して送信するとともに、ＵＲＬ２－１により特定される処理を実行する駅サーバ６－３との通信を要求する。個人サーバ５は、携帯端末２から送信されたデータを受信するとともに、その要求を認識する。個人サーバ５は、受信したデータを、ユーザＡの個人情報として記憶する。

【０２１０】

ステップＳ１１２の処理を具体的に説明すると、携帯端末２のＣＰＵ２１は、ステップＳ１１１で受信した情報を、表示部２４に表示させる。ユーザＡは、表示部２４に表示された情報を確認すると、入力部２３に対して所定の操作を行う。これにより、携帯端末２は、ステップＳ１１１で受信した情報を、個人サーバ５に送信する。

【０２１１】

ステップＳ１１３において、個人サーバ５と駅サーバ６－３との通信が確立されると、ステップＳ１１４において、個人サーバ５は、ステップＳ１１２で受信した入札時刻および駅ＡのＩＤを、ＵＲＬ１とともに、駅サーバ６－３に送信する。駅サーバ６－３は、それらを受信する。

【０２１２】

次に、ステップＳ１１５において、駅サーバ６－３は、個人サーバ５に対して、ユーザ認証を要求する。個人サーバ５は、その要求を認識する。

【０２１３】

ステップＳ１１６において、認証データによるユーザ認証が行われる。ここでの処理は、図６のステップＳ７における処理と同様であるので、その説明は省略する。

【０２１４】

ステップＳ１１６で、ユーザＡが正規のユーザであると認証されると、ステップＳ１１７において、駅サーバ６－３は、ステップＳ１１４で受信したデータを、記憶する。その後、処理は終了する。

【０２１５】

次に、出札処理の手順を、図２２のフローチャートを参照して説明する。

【０２１６】

ステップＳ１２１において、駅Ｂの改札機３－５は、ＵＲＬ２－２、出札時刻、および駅ＢのＩＤを、携帯端末２に送信する。携帯端末２は、それらを受信する。このとき、ユーザＡ（携帯端末２）は、携帯端末２と改札機３－５との短距離通信が可能となる程度に、改札機３－５に近づいているものとする。

【０２１７】

次に、ステップＳ１２２において、携帯端末２は、個人サーバ５に、ステップＳ１２１で受信したＵＲＬ２－２、出札時刻、および駅ＢのＩＤを、改札機３－５およびネットワーク４を介して送信するとともに、ＵＲＬ２－２により特定される処理を実行する駅サーバ６－４との通信を要求する。個人サーバ５は、携帯端末２から送信されたデータを受信するとともに、その要求を認識する。

【０２１８】

ステップＳ１２２の処理を具体的に説明すると、携帯端末２のＣＰＵ２１は、ステップＳ１２１で受信したデータを、表示部２４に表示させる。ユーザＡは、表示部２４に表示された情報を確認し、入力部２３に対して所定の操作を行う。これにより、携帯端末２は、ステップＳ１２１で受信した情報を、個人サーバ５に送信する。

【０２１９】

ステップＳ１２３において、個人サーバ５と駅サーバ６－４との通信が確立されると、ステップＳ１２４で、個人サーバ５は、ステップＳ１２２で受信した出札時刻および駅ＢのＩＤを、ＵＲＬ１とともに、駅サーバ６－４に送信する。駅サーバ６－４は、それらを受信する。

【０２２０】

ステップＳ１２５において、駅サーバ６－４は、個人サーバ５に対して、ユーザ認証を要求する。個人サーバ５は、その要求を認識する。

【０２２１】

次に、ステップＳ１２６において、認証データによるユーザ認証が行われる。ここでの処理は、図６のステップＳ７における処理と同様であるので、その説明は省略する。

【０２２２】

ステップＳ１２６で、ユーザＡが正規のユーザであると認証されると、ステップＳ１２７において、料金算出処理が行われる。ここでの処理は、図２３のフローチャートに示されている。

【０２２３】

ステップＳ１３１において、駅サーバ６－４は、個人サーバ５と通信し、ユーザＡの個人情報として記憶されている駅ＡのＩＤ（図２１のステップＳ１１２）を取得する。

【０２２４】

ステップＳ１３２において、駅サーバ６－４は、ステップＳ１３１で取得した駅ＡのＩＤと、ステップＳ１２４で受信した駅ＢのＩＤに基づいて、料金を算出する。その後、処理は終了し、図２２のステップＳ１２８に進む。

【０２２５】

ステップＳ１２８において、支払処理が行われる。駅サーバ６－４は、ステップＳ１２７で算出された料金の振り込み先を、個人サーバ５に通信する。個人サーバ５は、通知された振込先のサーバ（図示せず）に対して、所定の振り込み処理を行う。その後、処理は終了する。

【０２２６】

図２４は、本発明を適用したサービス提供システムの他の利用例を示している。この場合、サービス提供システムにより、遊園地のアトラクションを、１日に限って自由に利用することができる入場券（１日フリーチケット）の券売処理および改札処理（ゲート処理）が行われる。

【０２２７】

券売機３－６は、遊園地の入場券を発券する装置である。ゲート機３－７は、所定のアトラクション付近に設定されているゲートであり、そのアトラクションを行う場合は、ユーザＡは、必ずゲート機３－７のゲート（図示せず）を通過しなければならない。

【０２２８】

券売機３－６およびゲート機３－７は共に、ネットワークアクセスポートとしての機能を有し、チケットサーバ６－５およびゲートサーバ６－６とネットワーク４を介して通信する。

【０２２９】

チケットサーバ６－５は、ＵＲＬ２－１により特定される、発券した入場券に関する情報を管理する処理を実行し、ゲートサーバ６－６は、ＵＲＬ２－２により特定される、ゲート機３－７のゲートの開閉を制御する処理を実行する。

【０２３０】

次に、発券処理の手順を、図２５のフローチャートを参照して説明する。

【０２３１】

ステップＳ１４１において、券売機３－６は、ＵＲＬ２－１と、利用可能が日付等の、１日フリーチケットの利用に関する情報（以下、チケット情報）を、携帯端末２に送信する。携帯端末２は、それらを受信する。

【０２３２】

なお、このとき、ユーザＡは、券売機３－６の操作パネル（図示せず）に対して、１日フリーチケットを購入するための操作を行う。また、ユーザＡ（携帯端末２）は、携帯端末２と券売機３－６との短距離通信が可能となる程度に、券売機３－６に近づいているものとする。

【０２３３】

ステップＳ１４２において、携帯端末２は、個人サーバ５に、ステップＳ１４１で受信したＵＲＬ２－１およびチケット情報を送信するとともに、ＵＲＬ２－１により特定される処理を実行するチケットサーバ６－５との通信を要求する。個人サーバ５は、携帯端末２から送信されたデータを受信するとともに、その要求を認識する。

【０２３４】

ステップＳ１４２での処理を具体的に説明すると、携帯端末２のＣＰＵ２１は、ステップＳ１４２で受信した情報を、表示部２４に表示させる。ユーザＡは、表示部２４に表示された情報を確認すると、入力部２３に対して所定の操作を行う。これにより、携帯端末２は、その操作に基づいて、ステップＳ１４１で受信した情報を、個人サーバ５に送信する。

【０２３５】

ステップＳ１４３において、個人サーバ５とチケットサーバ６－５との通信が確立すると、ステップＳ１４４において、個人サーバ５は、ステップＳ１４２で受信したチケット情報を、ＵＲＬ１とともに、チケットサーバ６－５に送信する。チケットサーバ６－５は、それを受信する。

【０２３６】

ステップＳ１４５において、チケットサーバ６－５は、個人サーバ５に対して、ユーザ認証を要求する。個人サーバ５は、その要求を認識する。

【０２３７】

次に、ステップＳ１４６において、認証データによるユーザ認証が行われる。ここでの処理は、図６のステップＳ７における処理と同様であるので、その説明は省略する。

【０２３８】

ステップＳ１４６で、ユーザＡが正規のユーザであると認証されると、ステップＳ１４７において、発券処理が行われる。ここでの処理の詳細は、図２６のフローチャートに示されている。

【０２３９】

ステップＳ１５１において、チケットサーバ６－５は、ステップＳ１４４で受信したチケット情報に基づいて、有効期限を決定するとともに、料金を算出する。この例の場合、有効期限は、本日の終了時刻とされる。

【０２４０】

次に、ステップＳ１５２において、チケットサーバ６－５は、ステップＳ１５１で決定した有効期限を、ステップＳ１４４で受信したＵＲＬ１と対応させて記

憶する。

【０２４１】

ステップＳ１５３において、支払処理が行われる。チケットサーバ６－５は、ステップＳ１５１で算出した料金の振り込み先を、個人サーバ５に通信する。個人サーバ５は、通知された振り込み先のサーバ（図示せず）に対して、所定の振り込み処理を行う。

【０２４２】

ステップＳ１５３で、支払処理が完了すると、ステップＳ１５４において、チケットサーバ６－５は、ステップＳ１５１で決定した有効期限等からなるチケット情報を、個人サーバ５に送信する。個人サーバ５は、それを受信する。

【０２４３】

ステップＳ１５５において、個人サーバ５は、ステップＳ１５４で受信したチケット情報を、ユーザＡの個人情報として記憶する。

【０２４４】

その後、処理は終了し、図２５に戻り、発券処理が終了する。

【０２４５】

次に、ゲート処理の手順を、図２７のフローチャートを参照して説明する。

【０２４６】

ステップＳ１６１において、ゲート機３－７は、ＵＲＬ２－２を、携帯端末２に送信する。携帯端末２は、それを受信する。なお、このとき、ユーザＡは、携帯端末２とゲート機３－７との短距離通信が行われる程度にゲート機３－７に近づいているものとする。

【０２４７】

次に、ステップＳ１６２において、携帯端末２は、個人サーバ５に、ステップＳ１６１で受信したＵＲＬ２－２を送信するとともに、ＵＲＬ２－２により特定される処理を実行するゲートサーバ６－６との通信を要求する。個人サーバ５は、携帯端末２から送信されたＵＲＬ２－２を受信するとともに、その要求を認識する。

【０２４８】

ステップＳ１６３において、個人サーバ５とゲートサーバ６－６との通信が確立されると、ステップＳ１６４において、個人サーバ５は、図２６のステップＳ１５５で記憶したチケット情報を、ゲートサーバ６－６に送信する。ゲートサーバ６－６は、それを受信する。

【０２４９】

ステップＳ１６５において、ゲートサーバ６－６は、チケットサーバ６－５にアクセスし、ＵＲＬ１とともに記憶されている有効期限を取得し、それがステップＳ１６４で受信したチケット情報に示される有効期限と一致し、かつ、その期限が切れていないか否か判定する。すなわち、ユーザＡが、ゲート機３－７を通過できるか否かが判定される。

【０２５０】

ステップＳ１６５で、通過できると判定された場合、ステップＳ１６６に進み、ゲート機３－７のゲートが開放される。具体的には、ゲートサーバ６－６は、ゲートを開放させる指令を、ゲート機３－７に送信し、ゲート機３－７は、その指令に従い、ゲートを開放する。

【０２５１】

ステップＳ１６５で、通過できないと判定された場合、ステップＳ１６７に進み、ゲート機３－７のゲートは開放されず、所定のメッセージが出力される。

【０２５２】

ステップＳ１６６またはステップＳ１６７の後、ゲート処理は終了する。

【０２５３】

次に、ステップＳ１４７（発券処理）の他の処理について、図２８のフローチャートを参照して説明する。

【０２５４】

ステップＳ１７１において、チケットサーバ６－５は、図２５のステップＳ１４４で受信したチケット情報に基づいて、有効期限を決定するとともに、料金を算出する。

【０２５５】

次に、ステップＳ１７２において、チケットサーバ６－５は、ステップＳ１７

１で決定した有効期限を、ＵＲＬ１と対応させて記憶するとともに、ゲートサーバ６－６に送信する。ゲートサーバ６－６は、それを受信し、記憶する。

【０２５６】

ステップＳ１７３において、支払処理が行われる。

【０２５７】

次に、ステップＳ１７４において、個人サーバ５は、ユーザＡの顔写真データを、チケットサーバ６－５に送信する。チケットサーバ６－５は、それを受信する。

【０２５８】

ステップＳ１７５において、チケットサーバ６－５は、ステップＳ１７４で受信した顔写真データをＵＲＬ１と対応させて記憶するとともに、顔写真データを、ゲートサーバ６－６に送信する。ゲートサーバ６－６は、それを受信し、ＵＲＬ１と対応させて記憶する。

【０２５９】

その後、処理は終了する。

【０２６０】

次に、この発券処理に対応するゲート処理を、図２９のフローチャートを参照して説明する。

【０２６１】

ステップＳ１８１において、携帯端末２は、ＵＲＬ１を、ゲート機３－７を介してゲートサーバ６－６に送信する。ゲートサーバ６－６は、それを受信する。なお、ユーザＡは（携帯端末２）は、携帯端末２とゲート機３－７との短距離通信が可能となる程度にゲート機３－７に近づいているものとする。

【０２６２】

ステップＳ１８２において、ゲートサーバ６－６は、図２８のステップＳ１７２で記憶した有効期限を読み出し、ステップＳ１８３において、その有効期限が切れているか否かを判定する。すなわち、ユーザＡが、ゲート機３－７のゲートを通過することができるか否かが判定される。

【０２６３】

ステップＳ１８３で、通過できると判定された場合、ステップＳ１８４において、ゲートサーバ６－６は、ステップＳ１７５で記憶した顔写真データとともに、ゲートを開放する指令を、ゲート機３－７に送信する。

【０２６４】

ステップＳ１８５において、ゲート機３－７は、ステップＳ１８４で受信した顔写真データに対応する画像を表示するとともに、ゲートを開放する。

【０２６５】

ステップＳ１８３で、通過できないと判定された場合、ステップＳ１８６に進み、処理の処理が実行される。

【０２６６】

ステップＳ１８５またはステップＳ１８６の後、処理は終了する。

【０２６７】

なお、図２５の例では、認証データによるユーザ認証により、ユーザＡが正規のユーザであると認証された場合、チケットが発券される場合を例として説明したが、そのユーザ認証処理を省略することもできる。

【０２６８】

しなしながら、この場合、チケットサーバ６－５に記憶されたＵＲＬ１（図２６のステップＳ１５２）をユーザＡ以外の第３者が取得すれば、そのＵＲＬ１をゲート機３－７に送信することで（図２７のステップＳ１６１）、不正にゲート機３－７を通過することができる（不正にアトラクションを利用することができる）。

【０２６９】

図３０には、認証データによるユーザ認証が省略された場合でも不正利用を防止することができるシステムの構成例が示されている。

【０２７０】

通過監視装置３－８は、開放自在なゲート３－８Ａを有しており、ユーザが、図中矢印方向に移動する通路Ａの所定の地点Ａに設置されている。ユーザは、その通路を通る際、必ず通過監視装置３－８のゲート３－８Ａを通過しなければならない。

【０２７１】

通過監視装置３－８はまた、携帯端末２に対するネットワークアクセスポートとしての機能を有しており、携帯端末２と通信するとともに、ネットワーク４を介してチケットサーバ６－５および監視サーバ６－７と通信する。

【０２７２】

通過監視装置３－９は、通過監視装置３－８と同様に、開放自在なゲート３－９Ａを有しており、地点Ａから、図中矢印で示される進行方向に対して、所定の距離だけ離れた地点Ｂに設置されている。地点Ａと地点Ｂ間は、その間を移動するのに（歩くのに）、所定の時間以上かかる分だけ離れている。

【０２７３】

通過監視装置３－９も、携帯端末２に対するネットワークアクセスポートとしての機能を有しており、携帯端末２と通信し、ネットワーク４を介してチケットサーバ６－５および監視サーバ６－７と通信する。

【０２７４】

監視サーバ６－７は、ＵＲＬ２－３により特定される、通過監視装置３－９のゲート３－９Ａを通過しようとしているユーザが、チケットを不正利用しているか否かを監視する処理を実行する。

【０２７５】

次に、通過監視装置３－８の動作を、図３１のフローチャートを参照して説明する。

【０２７６】

ステップＳ１９１において、通過監視装置３－８は、ＵＲＬ２－３、検知時刻、および自分自身のＩＤを、携帯端末２に送信する。携帯端末２は、それを受信する。このとき、ユーザＡ（携帯端末２）は、携帯端末２と通過監視装置３－８との短距離通信が可能となる程度に、通過監視装置３－８に近づいている。

【０２７７】

次に、ステップＳ１９２において、携帯端末２は、個人サーバ５に、ステップＳ１９１で受信したＵＲＬ２－３、検知時刻、およびＩＤを、通過監視装置３－８を介して送信するとともに、ＵＲＬ２－３により特定される処理を実行する監

視サーバ６－７との通信を要求する。個人サーバ５は、携帯端末２から送信されたデータを受信するとともに、その要求を認識する。

【０２７８】

ステップＳ１９３において、個人サーバ５と監視サーバ６－７との通信が確立されると、ステップＳ１９４において、個人サーバ５は、ステップＳ１９２で受信した検知時刻およびＩＤを、ＵＲＬ１とともに、監視サーバ６－７に送信する。監視サーバ６－７は、それらを受信する。

【０２７９】

次に、ステップＳ１９５において、監視サーバ６－７は、ステップＳ１９４で受信した検知時刻、ＩＤ、およびＵＲＬ１をそれぞれ対応させて記憶する。

【０２８０】

ステップＳ１９６において、監視サーバ６－７は、チケットサーバ６－５と通信し、ステップＳ１９４で記憶したＵＲＬ１が、チケットサーバ６－５に管理されているか否かを判定する（図２６のステップＳ１５２の処理で、ＵＲＬ１が記憶されているか否かを判定する）。すなわち、ユーザＡが、正規にチケットを購入し、ゲート３－８Ａを通過することができる者であるか否かが判定される。

【０２８１】

ステップＳ１９６で、通過することができる者であると判定された場合、ステップＳ１９７に進む。

【０２８２】

ステップＳ１９７において、監視サーバ６－７は、通過監視装置３－８のゲート３－８Ａを開放させる処理を行う。これにより、そのゲート３－８Ａが開放し、ユーザＡは、そこを通過することができる。

【０２８３】

ステップＳ１９６で、通過することができない者であると判定された場合、ステップＳ１９８に進み、監視サーバ６－７は、所定の警告処理を実行する。

【０２８４】

ステップＳ１９７またはステップＳ１９８での処理が行われた後、通過監視処理は終了する。

【０２８５】

次に、通過監視装置３－９の動作を、図３２のフローチャートを参照して説明する。

【０２８６】

ステップＳ２０１において、通過監視装置３－９は、ＵＲＬ２－３、検知時刻、および自分自身のＩＤを、携帯端末２に送信する。携帯端末２は、それらを受信する。このとき、ユーザＡ（携帯端末２）は、携帯端末２と通過監視装置３－９との短距離通信が可能となる程度に、通過監視装置３－９に近づいている。

【０２８７】

次に、ステップＳ２０２において、携帯端末２は、個人サーバ５に、ステップＳ２０１で受信したＵＲＬ２－３、検知時刻、およびＩＤを、通過監視装置３－９を介して送信するとともに、ＵＲＬ２－３により特定される処理を実行する監視サーバ６－７との通信を要求する。個人サーバ５は、携帯端末２から送信されたデータを受信するとともに、その要求を認識する。

【０２８８】

ステップＳ２０３において、個人サーバ５と監視サーバ６－７との通信が確立されると、ステップＳ２０４において、個人サーバ５は、ステップＳ２０２で受信した検知時刻およびＩＤを、ＵＲＬ１とともに、監視サーバ６－７に送信する。監視サーバ６－７は、それを受信する。

【０２８９】

次に、ステップＳ２０５において、監視サーバ６－７は、図３１のステップＳ１９５でＵＲＬ１と対応して記憶した、通過監視装置３－８での検知時刻を読み出し、ステップＳ２０６において、ステップＳ２０４で受信した検知時刻との差（時間）を算出し、その時間が、予め決められた時間（地点Ａから地点Ｂに移動するのに必要な時間）Ｔより短いか否かを判定する。

【０２９０】

通過監視装置３－８と通過監視装置３－９は、移動するのに時間Ｔかかるだけ離れているので、ユーザＡが、通過監視装置３－８（ゲート３－８Ａ）を通過した後、時間Ｔ以内に、通過監視装置３－９により検知される場合はない。すなわ

ち、時間Ｔ以内に、ＵＲＬ１が通過監視装置３－９に送信された場合、ＵＲＬ１が、第３者により不正に保持されているものとすることができる。従って、ここでの処理では、ＵＲＬ１が不正利用されているか否かが判定され、ユーザＡがゲート３－９Ａを通過することができる者であるか否かが判定される。

【０２９１】

ステップＳ２０６で、通過することができる者であると判定された場合、ステップＳ２０７に進み、監視サーバ６－７は、通過監視装置３－９のゲート３－９Ａを開放させる処理を行う。これにより、ゲート３－９Ａが開放し、ユーザＡは、そこを通過することができる。

【０２９２】

ステップＳ２０６で、通過することができない者であると判定された場合、ステップＳ２０８に進み、監視サーバ６－７は、所定の警告処理を実行する。

【０２９３】

ステップＳ２０７またはステップＳ２０８での処理が行われた後、この通過監視処理は終了する。

【０２９４】

図３３は、本発明を適用したサービス提供システムの他の利用例を示している。この場合は、サービス提供システムにより、有料道路の通行料金の支払処理が行われる。ユーザＡは、携帯端末２を携帯して自動車Ａに搭乗している。

【０２９５】

入門ゲート機３－１０は、携帯端末２に対するネットワークアクセスポートとしての機能を有する装置で、有料道路の入口に設置されている。

【０２９６】

料金ゲート機３－１１は、携帯端末２に対するネットワークアクセスポートとしての機能を有する装置で、有料道路の出口に設置されている。料金ゲート機３－１１はまた、ビデオカメラ（図示せず）を有し、通過する自動車の車両番号を撮像するとともに、その結果得られた画像データから、車両番号を検出する。

【０２９７】

通行料金サーバ６－８は、個人サーバ５、入門ゲート機３－１０、または料金

サーバ３－１１と、ネットワーク４を介して通信し、ＵＲＬ２により特定される、有料道路の通行料金の支払に関する処理を実行する。通行料金サーバ６－８は、自動車（自動車Ａ）の車両番号を、所定の有効期限とともに予め記憶している。

【０２９８】

個人サーバ５は、ユーザＡの自動車の車両番号を、ユーザＡの個人情報として記憶している。

【０２９９】

次に、この支払処理の手順を、図３４のフローチャートを参照して説明する。

【０３００】

ステップＳ２２１において、携帯端末２は、ＵＲＬ１を、入門ゲート機３－１０に送信する。入門ゲート機３－１０は、それを受信する。

【０３０１】

具体的には、自動車Ａ（携帯端末２）が、携帯端末２と入門ゲート機３－１０との短距離通信が可能となる程度にまで、入門ゲート機３－１０に近づいたとき、ユーザＡは、携帯端末２の入力部２３に対して所定の操作を行う。これにより、携帯端末２は、上記したデータを、入門ゲート機３－１０に送信する。

【０３０２】

次に、ステップＳ２２２において、入門ゲート機３－１０は、ステップＳ２２１で受信したＵＲＬ１とその受信時刻を、通行料金サーバ６－８に送信する。通行料金サーバ６－８は、それらを受信する。

【０３０３】

ステップＳ２２３において、通行料金サーバ６－８は、ステップＳ２２２で受信したＵＲＬ１と受信時刻を記憶する。

【０３０４】

次に、ステップＳ２２４において、携帯端末２は、ＵＲＬ１を、料金ゲート機３－１１に送信する。料金ゲート機３－１１は、それを受信する。

【０３０５】

自動車Ａは、有路道路を走行し、料金ゲート機３－１１が設置されている出口

から降り、料金ゲート機３－１１に近づいたとき（携帯端末２と料金ゲート機３－１１との短距離通信が可能となる程度にまで近づいたとき）、ユーザＡは、携帯端末２の入力部２３に対して所定の操作を行う。これにより、携帯端末２は、ＵＲＬ１を、料金ゲート機３－１１に送信する。

【０３０６】

ステップＳ２２５において、料金ゲート機３－１１は、通過する自動車Ａを撮像し、その結果得られた画像データから車両番号を検出する。料金ゲート機３－１１は、検出した車両番号を、ステップＳ２２４で受信したＵＲＬ１とその受信時刻とともに、通行料金サーバ６－８に送信する。通行料金サーバ６－８は、それらを受信する。

【０３０７】

ステップＳ２２６において、通行料金サーバ６－８は、自動車Ａが料金ゲート機３－１１を通過することができるか否かを判定する。

【０３０８】

この例の場合、個人サーバ５と通行料金サーバ６－８の間において、ユーザＡに対する、認証データによるユーザ認証（例えば、図６のステップＳ７）が予め行われており、通行料金サーバ６－８は、ユーザＡが正規のユーザである情報を、その情報の有効期限、および車両番号とともに、ＵＲＬ１に対応させて記憶している。すなわち、ここでの処理（ステップＳ２２６）で、通行料金サーバ６－８は、ステップＳ２２５で受信した車両番号と、ＵＲＬ１と対応させて予め記憶している車両番号とを照合し、同一であるか否かを判定し、またステップＳ２２３で記憶した受信時刻が、ＵＲＬ１と対応させて予め記憶している有効期限内の時刻を示しているか否かを判定する。従って、車両番号が同一であり、かつ、有効期限内であると判定されたとき、自動車Ａは、料金ゲート機３－１１を通過することができるものと判定され、ステップＳ２２７に進み、支払処理が行われる。

【０３０９】

一方、ステップＳ２２６で、車両番号が同一ではなく、または有効期限内ではないと判定された場合、自動車Ａは、料金ゲート機３－１１を通過することがで

きないものと判定され、ステップＳ２２８に進み、所定の警告処理が行われる。

【０３１０】

図３５は、本発明を適用したサービス提供システムの他の利用例を示している。この場合は、サービス提供システムにより、公共料金の精算処理が行われる。

【０３１１】

精算装置３－１２は、公共料金に関する契約または精算をする場合に操作される端末で、例えば、コンビニエンスストアー等に設置されている。精算装置３－１２はまた、携帯端末２に対するネットワークアクセスポートとしての機能を有している。

【０３１２】

公共料金サーバ６－９は、ネットワーク４を介して、精算装置３－１２および個人サーバ５と通信し、ＵＲＬ２により特定される公共料金に関する処理を実行する。

【０３１３】

次に、このシステムを利用して公共料金の精算を行うための契約処理の手順を、図３６のフローチャートを参照して説明する。

【０３１４】

ステップＳ２４１において、精算装置３－１２は、ＵＲＬ２と契約情報を、携帯端末２に送信する。携帯端末２は、それを受信する。

【０３１５】

このとき、ユーザＡは、精算装置３－１２に対して、例えば、自分の名前など、契約情報を入力する操作を行う。これにより、精算装置３－１２は、上述した情報を、携帯端末２に送信する。

【０３１６】

次に、ステップＳ２４２において、携帯端末２は、個人サーバ５に、ステップＳ２４１で受信したＵＲＬ２と契約情報を、精算装置３－１２およびネットワーク４を介して送信するとともに、公共料金サーバ６－９との通信を要求する。

【０３１７】

ステップＳ２４３において、個人サーバ５と公共料金サーバ６－９との通信が

確立される。

【０３１８】

次に、ステップＳ２４４において、個人サーバ５は、ステップＳ２４２で受信した契約情報を、公共料金サーバ６－９に送信する。公共料金サーバ６－９は、それを受信する。

【０３１９】

ステップＳ２４５において、公共料金サーバ６－９は、ユーザ認証を、個人サーバ５に要求する。個人サーバ５は、その要求を認識する。

【０３２０】

ステップＳ２４６において、ユーザ認証が行われる。ここでの処理は、図６のステップＳ７における処理と同様であるので、その説明は省略する。

【０３２１】

次に、ステップＳ２４７において、契約処理が行われる。この処理の詳細は、図３７にフローチャートに示されている。

【０３２２】

ステップＳ２５１において、公共料金サーバ６－９は、ステップＳ２４４で受信した契約情報に基づいて、契約期限を決定する。

【０３２３】

ステップＳ２５２において、公共料金サーバ６－９は、ステップＳ２５１で決定した契約期限をＵＲＬ１に対応させて記憶するとともに、契約期限とＵＲＬ２を、個人サーバ５に送信する。個人サーバ５は、それを受信する。

【０３２４】

ステップＳ２５３において、個人サーバ５は、ステップＳ２５２で受信したＵＲＬ２と契約期限を記憶する。その後処理は、終了する。

【０３２５】

次に、公共料金の精算処理を、図３８のフローチャートを参照して説明する。

【０３２６】

ステップＳ２６１において、個人サーバ５と公共料金サーバ６－９との通信が確立される。具体的には、公共料金サーバ６－９は、予め決められたタイミング

（例えば、毎月所定の日）に、個人サーバ５に対して、接続を要求する。個人サーバ５は、それに応答する。

【０３２７】

ステップＳ２６２において、公共料金サーバ６－９は、公共料金の支払を、個人サーバ５に要求する。

【０３２８】

次に、ステップＳ２６３において、個人サーバ５は、ＵＲＬ２と対応して記憶した契約期限を参照し、それが切れているか否かを判定し、切れていないと判定した場合、ステップＳ２６４に進む。

【０３２９】

ステップＳ２６４において、支払処理が行われる。具体的には、個人サーバ５は、料金の振り込みサーバに対して振り込み処理を行う。個人サーバ５は、振り込み結果を、公共料金サーバ６－９に送信する。公共料金サーバ６－９は、それを記録する。

【０３３０】

ステップＳ２６３で、契約期限が切れていると判定された場合、ステップＳ２６５に進み、所定の処理が実行される。

【０３３１】

ステップＳ２６４またはステップＳ２６５の後、公共料金の支払処理は終了する。

【０３３２】

図３９は、本発明を適用したサービス提供システムの他の利用例を示している。この場合、サービス提供システムを利用により、病院におけるカルテ（診療簿）が管理される。

【０３３３】

カルテ管理端末３－１３は、カルテの内容を参照したいときに操作される端末で、例えば、病院内に設置されている。カルテ管理端末３－１３はまた、携帯端末２に対するネットワークアクセスポートとしての機能を有している。

【０３３４】

カルテ管理サーバ６－１０は、ネットワーク４を介して、カルテ管理端末３－１３および個人サーバ５と通信し、ＵＲＬ２により特定される、カルテ情報を管理する処理を実行する。

【０３３５】

次に、このシステムを利用したカルテ情報を参照するための処理手順を、図４０のフローチャートを参照して説明する。

【０３３６】

ステップＳ２７１において、カルテ管理端末３－１３は、ＵＲＬ２を、携帯端末２に送信する。携帯端末２は、それを受信する。

【０３３７】

ステップＳ２７２において、携帯端末２は、個人サーバ５は、ステップＳ２７１で受信したＵＲＬ２を、カルテ管理端末３－１３およびネットワーク４を介して送信するとともに、カルテ管理サーバ６－１０との通信を要求する。

【０３３８】

ステップＳ２７３において、個人サーバ５とカルテ管理サーバ６－１０との通信が確立される。

【０３３９】

次に、ステップＳ２７４において、カルテ管理サーバ６－１０は、個人サーバ５に対して、ユーザ認証を要求する。個人サーバ５は、その要求を認識する。

【０３４０】

ステップＳ２７５において、認証データによるユーザ認証が行われる。ここでの処理は、図６のステップＳ７における場合と同様であるので、その説明は省略する。

【０３４１】

ステップＳ２７５で、ユーザＡが正規のユーザであると認証されると、ステップＳ２７６において、カルテ管理サーバ６－１０は、ユーザ認証されたユーザＡのカルテ情報を、ＵＲＬ１の公開鍵で暗号化し、個人サーバ５に送信する。個人サーバ５は、それを受信する。なお、ＵＲＬ１の公開鍵は、ステップＳ２７５における処理で、個人サーバ５からカルテ管理サーバ６－１０に供給される。

【０３４２】

次に、ステップＳ２７７において、個人サーバ５は、ステップＳ２７６で受信したカルテ情報（ＵＲＬ１の公開鍵で暗号化されている）を、ＵＲＬ１の秘密鍵で解凍した後、携帯端末２の公開鍵で暗号化する。

【０３４３】

ステップＳ２７８において、個人サーバ５は、ステップＳ２７７で暗号化したカルテ情報を、カルテ管理端末３－１３を介して、携帯端末２に送信する。携帯端末２は、それを受信する。

【０３４４】

次に、ステップＳ２７９において、携帯端末２は、ステップＳ２７８で受信したカルテ情報（携帯端末２の公開鍵で暗号化されている）を、携帯端末２の秘密鍵で解凍し、それを表示部２４に表示する。これにより、ユーザＡは、自分のカルテの内容を知ることができる。

【０３４５】

その後、処理は終了する。

【０３４６】

図４１は、本発明を適用したサービス提供システムの他の利用例を示している。この例では、個人サーバ５、計算サーバ６－１１、表示装置６－１２、キーボード６－１３、およびマウス６－１４は、それぞれネットワークアクセスポート３およびネットワーク４を介して互いに接続し、いわゆるコンピュータを構成する。

【０３４７】

携帯端末２は、表示装置６－１２、キーボード６－１３、およびマウス６－１４と、例えば、赤外線通信等を行い、それぞれが管理するＵＲＬ２－２、ＵＲＬ２－３、およびＵＲＬ２－４を取得する。携帯端末２は、取得したＵＲＬ２－２、ＵＲＬ２－３、およびＵＲＬ２－４の他、コンピュータにおけるＣＰＵ的役割を果たす計算サーバ６－１１が管理するＵＲＬ２－１を、個人サーバ５に送信するとともに、これらのＵＲＬに基づく情報の伝達の制御を、個人サーバ５に要求する。これにより、ユーザＡによる、キーボード６－１３およびマウス６－１４

に対する操作に対応して、各種情報が、計算サーバ６－１１乃至マウス６－１４の間で送受信されるので、ユーザは、あたかも１台のコンピュータを利用している場合と同様に、例えば、計算処理等を行うことができる。

【０３４８】

なお、表示装置６－１２、キーボード６－１３、またはマウス６－１４が、ユーザＡがよく使用するものである場合、それらが管理するＵＲＬ２を、個人サーバ５が、ユーザＡの個人情報として記憶しておけば、新たにそれらのＵＲＬを取得する必要がなくなる。

【０３４９】

また、ユーザＡが、表示装置６－１２の前にいる場合のみ利用できるようにすることができる。この場合、携帯端末２は、ＵＲＬ１を、表示装置６－１２に転送し、表示装置６－１２は、受信したＵＲＬ１からの制御による場合のみ表示データ等を受信することができるようにする。

【０３５０】

このように、図４１に示したような利用例によれば、コンピュータの本体がなくても、表示装置や入力装置さえあれば、コンピュータとしての機能を利用することができる。

【０３５１】

ところで、コンピュータ上において実行される文書作成プログラムは、頻度良く入力される言葉または文書が記憶され、キー入力により、その言葉または文書の途中までの文字が入力されると、その言葉または文書の全体が出力される機能を有する。従って、この機能により、ユーザは、その言葉または文書の全ての文字をキー入力する必要がないので、文書作成等を容易に行うことができる。

【０３５２】

そこで、例えば、図４１の例の場合、そのような情報を、個人サーバ５が保持するようにし、必要に応じて、携帯端末２がそれを取得し、記憶することで、言葉や文書の全ての文字をキー入力しなくても、言葉や文書の全体を出力させることができる。

【０３５３】

なお、以上においては、携帯端末２に対するネットワークアクセスポート３は、所定の場所に固定されている場合を例として接続したが、図４２に示すように、ユーザＡが携帯する携帯電話（またはＰＨＳ）３－１４を、ネットワークアクセスポートとして利用することができる。この場合、携帯端末２と、例えば、個人サーバ５との通信は、携帯電話３－１４、基地局８１、公衆電話網８２、プロバイダ８３、およびネットワーク４を介して行われる。

【０３５４】

また、図４２の例では、携帯電話３－１４は、携帯端末２に対するネットワークアクセスポートとして利用されるが、図４３に示すように、携帯端末２としても利用することができる。なお、この場合、携帯電話３－１４は、腕時計１の認証データ用ＩＣチップと通信することができる機能を有している。

【０３５５】

上述した一連の処理は、ハードウエアにより実現させることもできるが、ソフトウエアにより実現させることもできる。一連の処理をソフトウエアにより実現する場合には、そのソフトウエアを構成するプログラムがコンピュータにインストールされ、そのプログラムがコンピュータで実行されることより、上述した、携帯端末２、個人サーバ５、またはサービスサーバ６－１等が機能的に実現される。

【０３５６】

図４４は、上述のような携帯端末２、個人サーバ５、またはサービスサーバ６－１等として機能するコンピュータ５０１の一実施の形態の構成を示すブロック図である。CPU５１１にはバス５１５を介して入出力インタフェース５１６が接続されており、CPU５１１は、入出力インタフェース５１６を介して、ユーザから、キーボード、マウスなどよりなる入力部５１８から指令が入力されると、例えば、ROM５１２、ハードディスク５１４、またはドライブ５２０に装着される磁気ディスク５３１、光ディスク５３２、光磁気ディスク５３３、若しくは半導体メモリ５３４などの記録媒体に格納されているプログラムを、RAM５１３にロードして実行する。これにより、上述した各種の処理が行われる。さらに、CPU５１１は、その処理結果を、例えば、入出力インタフェース５１６を介して、LC

Dなどよりなる表示部５１７に必要に応じて出力する。なお、プログラムは、ハードディスク５１４やROM５１２に予め記憶しておき、コンピュータ５０１と一体的にユーザに提供したり、磁気ディスク５３１、光ディスク５３２、光磁気ディスク５３３，半導体メモリ５３４等のパッケージメディアとして提供したり、衛星、ネットワーク等から通信部５１９を介してハードディスク５１４に提供することができる。

【０３５７】

なお、本明細書において、記録媒体により提供されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０３５８】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０３５９】

【発明の効果】

本発明の情報処理装置および方法、並びに記録媒体によれば、第１のネットワーク特定情報を記憶し、第２のネットワーク特定情報を取得し、ユーザを認証するために必要な認証データを取得し、取得された第２のネットワーク特定情報により特定される処理がサービスサーバにより実行されることで、サービスの提供を受けることができるように、第１のネットワーク特定情報により特定される個人情報を管理する個人サーバに、第１のネットワーク特定情報および第２のネットワーク特定情報を含む制御情報を送信するようにしたので、例えば、情報処理装置を紛失しても、個人情報が第３者に渡ることを防止することができる。

【０３６０】

本発明の第１のサービス提供システムによれば、携帯端末が、第１のネットワーク特定情報を記憶し、第２のネットワーク特定情報を取得し、ユーザを認証するために必要な認証データを取得し、取得された第２のネットワーク特定情報により特定される処理が第２のサーバにより実行されることで、所定のサービスの

提供を受けることができるように、記憶されている第１のネットワーク特定情報により特定される個人情報を管理する第１のサーバに、第１のネットワーク特定情報および第２のネットワーク特定情報を含む制御情報を供給し、取得された認証データを、第１のサーバに供給し、第１のサーバが、第１のネットワーク特定情報により特定される個人情報を管理し、供給された制御情報に含まれる第２のネットワーク特定情報により特定される処理を実行する第２のサーバに、制御情報および個人情報に基づくサービスの提供を要求し、第２のサーバからの要求に基づいて、供給された認証データに基づきユーザを認証し、認証結果を、第２のサーバに供給し、第２のサーバが、第２のネットワーク特定情報により特定される処理を管理し、要求があったとき、ユーザの認証を第１のサーバに要求し、供給された認証結果が、ユーザが、第１のサービス提供システムの正規のユーザである旨を示しているとき、第２のネットワーク特定情報により特定される処理を、制御情報および個人情報に基づいて実行するようにしたので、例えば、情報処理装置を紛失しても、個人情報が第３者に渡ることを防止することができる。

【０３６１】

本発明の第２のサービス提供システムによれば、携帯端末が、第１のネットワーク特定情報を記憶し、第２のネットワーク特定情報およびアクセスパターン検出のためのアクセス情報を、サービス端末から取得し、取得された第２のネットワーク特定情報により特定される処理が第２のサーバにより実行されることで、所定のサービスの提供を受けることができるように、記憶されている第１のネットワーク特定情報により特定される個人情報を管理する第１のサーバに、第１のネットワーク特定情報、第２のネットワーク特定情報、およびアクセス情報を含む制御情報を、サービス端末に供給し、サービス端末が、第２のネットワーク特定情報を保持し、自分自身に対するアクセスから、アクセス情報を取得し、取得されるように、第２のネットワーク特定情報およびアクセス情報を、携帯端末に供給し、供給された制御情報を、第１のサーバに供給し、第１のサーバが、第１のネットワーク特定情報により特定される個人情報を管理し、供給された制御情報に含まれる第２のネットワーク特定情報により特定される処理を実行する第２のサーバに、制御情報、個人情報、およびアクセス情報に基づくサービスの提供

を要求し、第２のサーバが、第２のネットワーク特定情報により特定される処理を管理し、要求に基づいて、第２のネットワーク特定情報により特定される処理を、制御情報、個人情報、およびアクセス情報に基づいて実行するようにしたので、例えば、情報処理装置を紛失しても、個人情報が第３者に渡ることを防止することができる。

【図面の簡単な説明】

【図１】

本発明を適用したサービス提供システムの利用例を示す図である。

【図２】

図１の腕時計１に組み込まれた認証データ用ＩＣチップの構成例を示すブロック図である。

【図３】

図１の携帯端末２の構成例を示すブロック図である。

【図４】

図１の精算装置３－１の構成例を示すブロック図である。

【図５】

図１の個人サーバ５の構成例を示すブロック図である。

【図６】

精算処理を説明するフローチャートである。

【図７】

図６のステップＳ６の処理を説明するフローチャートである。

【図８】

図６のステップＳ７の処理を説明するフローチャートである。

【図９】

携帯端末２の他の構成例を示すブロック図である。

【図１０】

商品券を利用した精算処理を説明するフローチャートである。

【図１１】

図１０のステップＳ４７の処理を説明するフローチャートである。

【図１２】

携帯端末２の他の構成例を示すブロック図である。

【図１３】

精算処理を説明する他のフローチャートである。

【図１４】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図１５】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図１６】

ネットショッピング処理を説明するフローチャートである。

【図１７】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図１８】

システム使用料の精算処理を説明するフローチャートである。

【図１９】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図２０】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図２１】

入札処理を説明するフローチャートである。

【図２２】

出札処理を説明するフローチャートである。

【図２３】

図２２のステップＳ１２７の処理を説明するフローチャートである。

【図２４】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図２５】

発券処理を説明するフローチャートである。

【図２６】

図２５のステップＳ１４７の処理を説明するフローチャートである。

【図２７】

ゲート処理を説明するフローチャートである。

【図２８】

図２５のステップＳ１４７の他の処理を説明するフローチャートである。

【図２９】

他のゲート処理を説明するフローチャートである。

【図３０】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図３１】

通過監視処理を説明するフローチャートである。

【図３２】

他の通過監視処理を説明するフローチャートである。

【図３３】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図３４】

有料道路の料金自動支払処理を説明するフローチャートである。

【図３５】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図３６】

契約処理を説明するフローチャートである。

【図３７】

図３６のステップＳ２４７の処理を説明するフローチャートである。

【図３８】

他の精算処理を説明するフローチャートである。

【図３９】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図４０】

カルテ管理処理を説明するフローチャートである。

【図４１】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図４２】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図４３】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図４４】

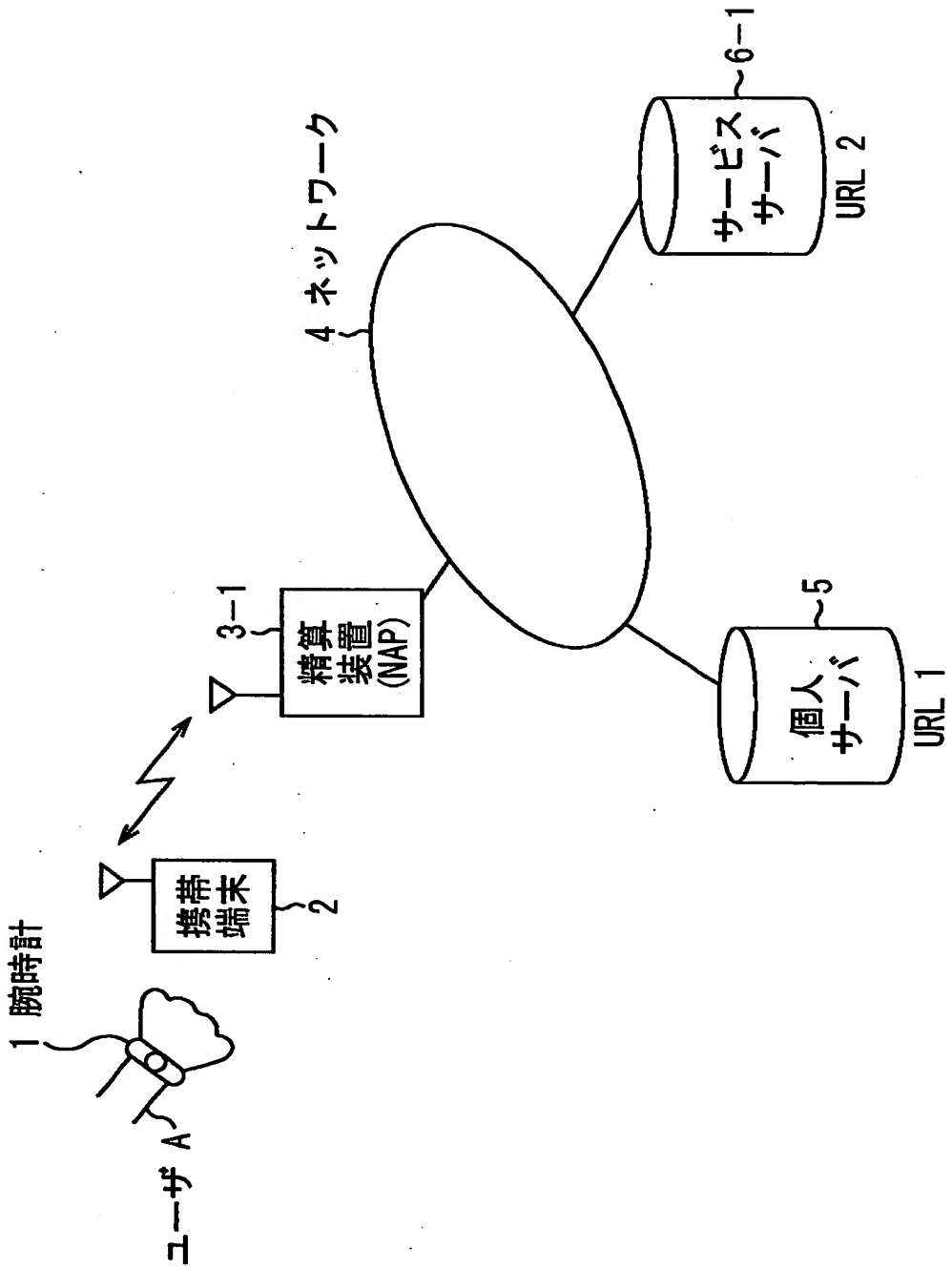
コンピュータ５０１の構成例を示すブロック図である。

【符号の説明】

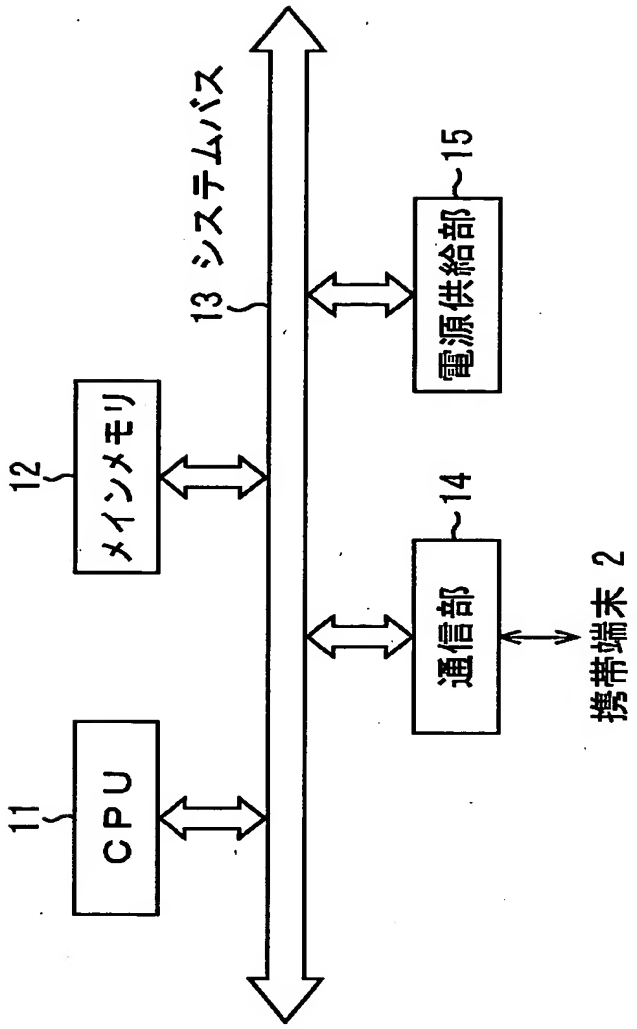
１　腕時計，　２　携帯端末，　３－１　精算装置，　３－２　モニター，３－３　パーソナルコンピュータ，　３－４　改札機，　３－５　改札機，３－６　券売機、　３－７　ゲート機，　３－８　通過監視装置，　３－９通過監視装置，　３－１０　入門ゲート機，　３－１１　料金ゲート機，　３－１２　精算装置，　３－１３　カルテ管理端末，　３－１４　携帯電話，　４ネットワーク，　５　個人サーバ，　６－１　サービスサーバ，　６－２　ショッピングサーバ，　６－３　駅サーバ，　６－４　駅サーバ，　６－５　チケットサーバ，　６－６　ゲートサーバ，　６－７　監視サーバ，　６－８　通行料金サーバ，　６－９　公共料金サーバ，　６－１０　カルテ管理サーバ，　６－１１　計算サーバ，　１１　ＣＰＵ，　１２　メインメモリ，　１３　システムバス，　１４　通信部，　１５　電源供給部，　２１　ＣＰＵ，　２２　メインメモリ，　２３　入力部，　２４　表示部，　２５　出力部，　２６　通信部，２７　通信部，　２８　インターフェース，　３１　ＣＰＵ，　３２　ＲＯＭ，　３３　ＲＡＭ，　３４　入力部，　３５　表示部，　３６　ハードディスク，　３７　通信部，　３８　通信部，　３９　インターフェース，　４１　ＣＰＵ，　４２　ＲＯＭ，　４３　ＲＡＭ，　４４　入力部，　４５　表示部，４６　ハードディスク，　４７　通信部，　４８　インターフェース，　５１指紋採取センサ，　５２　マイクロフォン，　６１　イメージセンサ，　７１管理サーバ

【書類名】図面

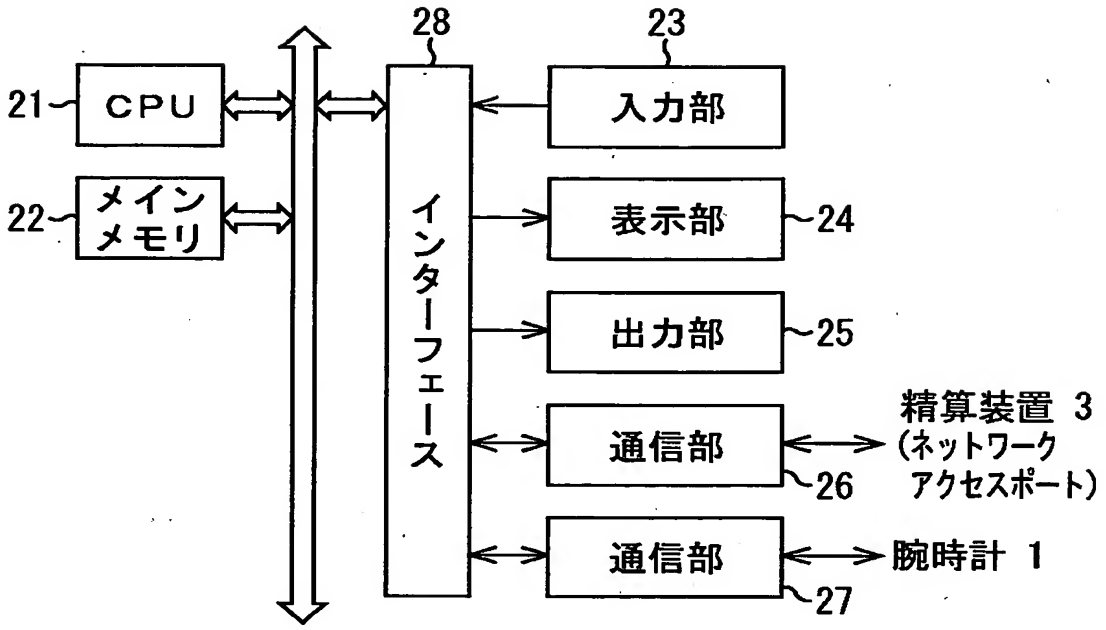
【図１】


1 腕時計
ユーザ A
2 携帯装置
3-1 精算装置 (NAP)
4 ネットワーク
5 個人サーバ URL 1
6-1 サービスサーバ URL 2

【図２】

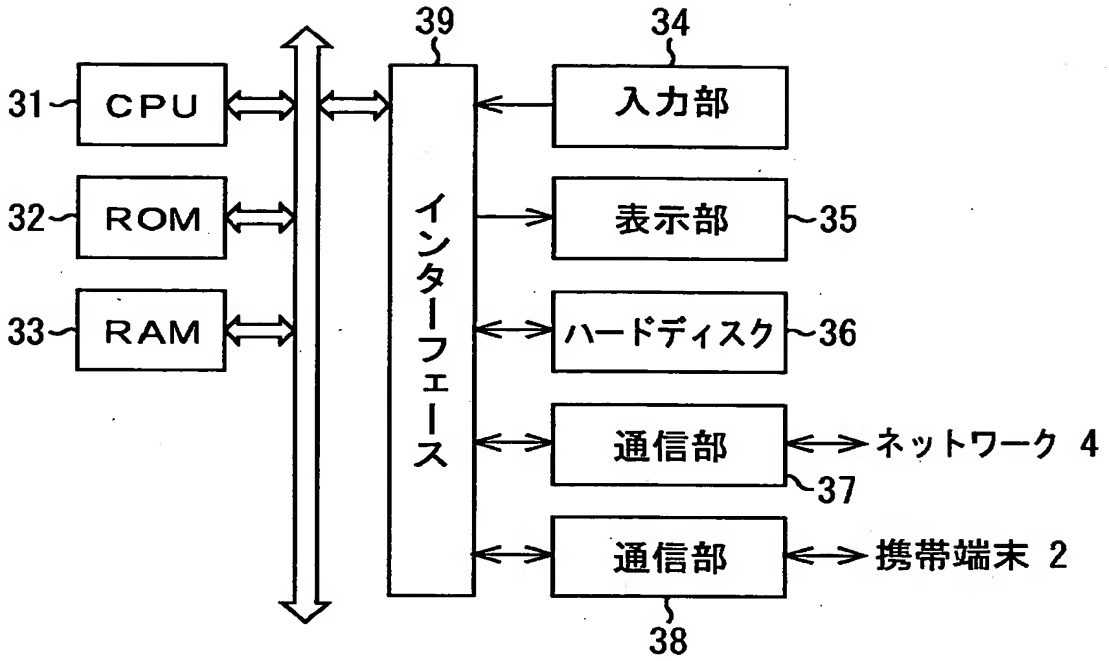

13 システムバス
11
CPU
12
メインメモリ
14
通信部
15
電源供給部
携帯端末 2
腕時計 1(認証データ用ICチップ)

【図３】


28
23
21
CPU
入力部
22
メイン
メモリ
インターフェース
表示部
24
出力部
25
精算装置 3
(ネットワーク
アクセスポート)
通信部
26
通信部
腕時計 1
27

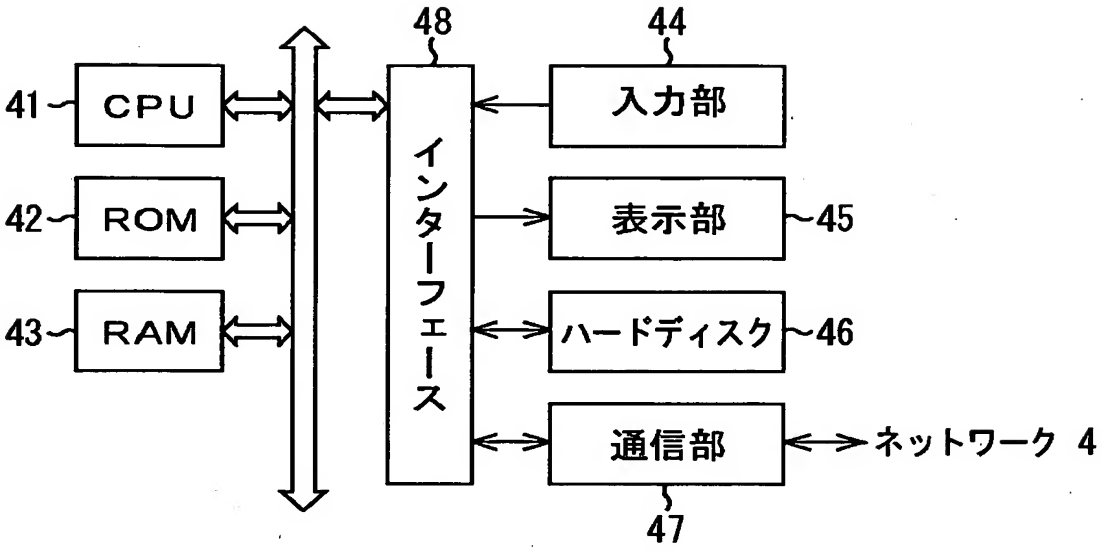
携帯端末 2

【図４】


39
34
31
CPU
32
ROM
33
RAM
インターフェース
入力部
表示部
35
ハードディスク
36
通信部
ネットワーク 4
37
通信部
携帯端末 2
38

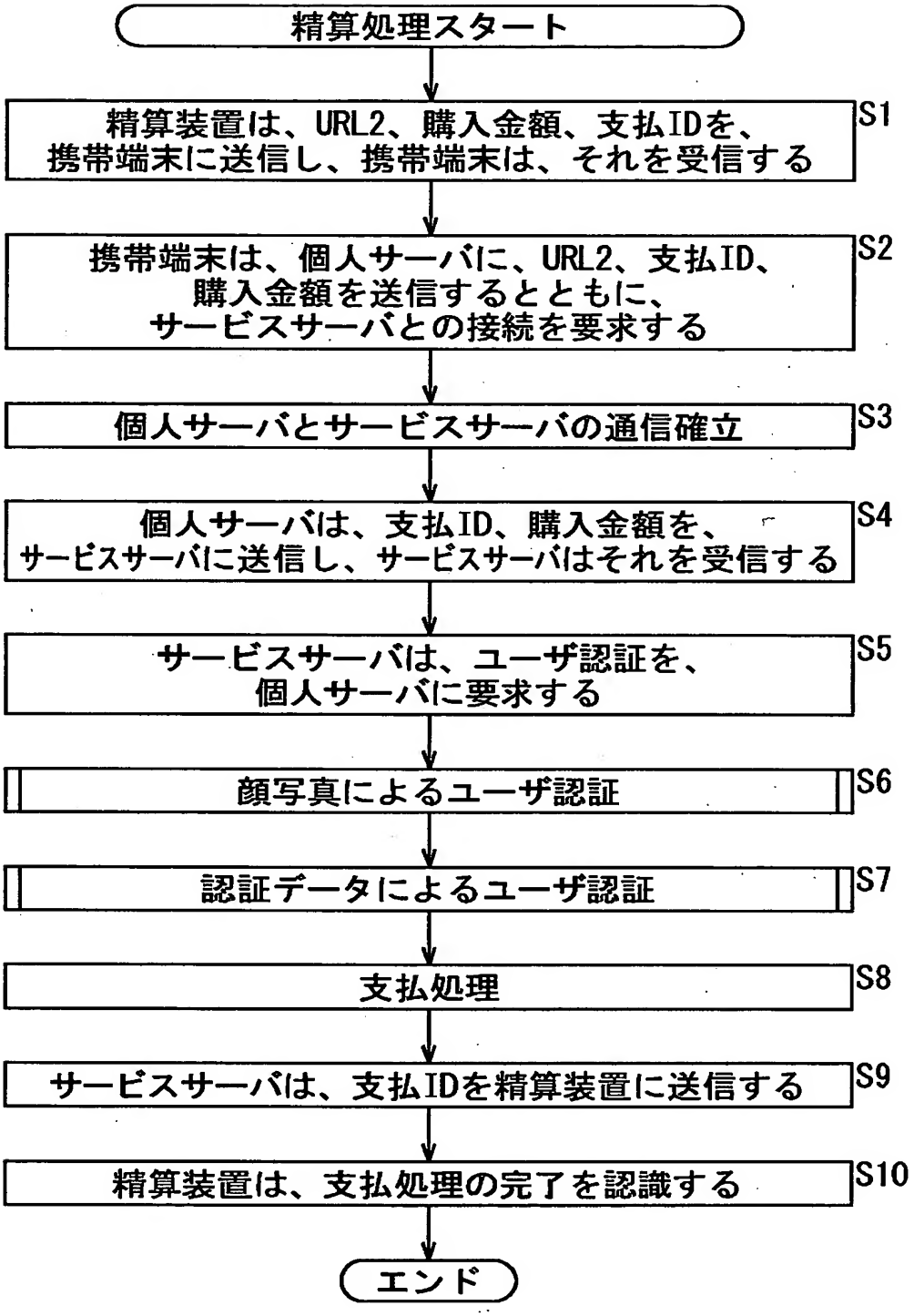
精算装置 3−1

【図５】

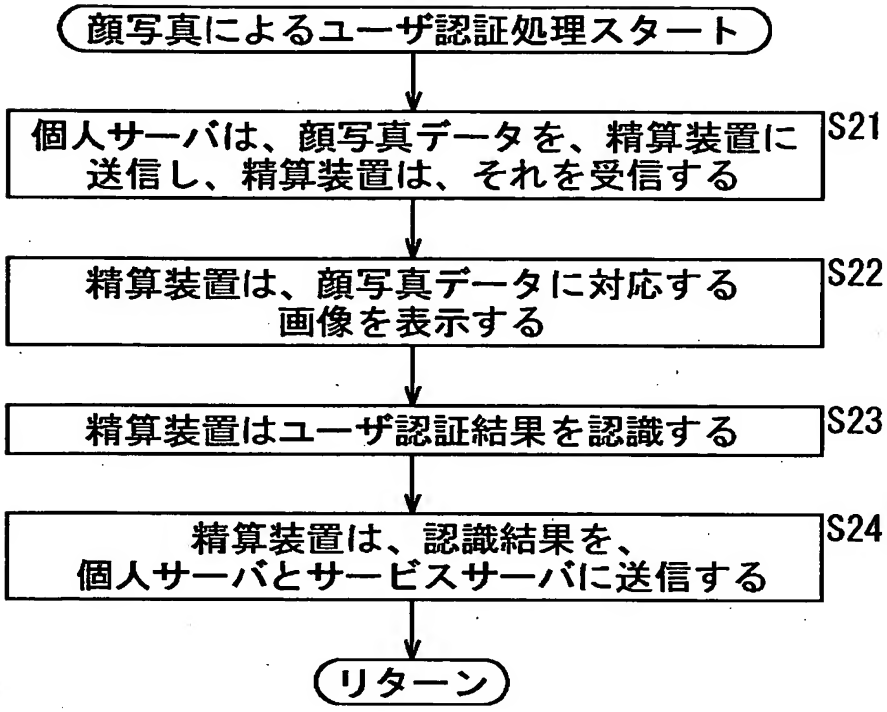

48
44
41
CPU
42
ROM
43
RAM
インターフェース
入力部
表示部
45
ハードディスク
46
通信部
ネットワーク 4
47

個人サーバ５

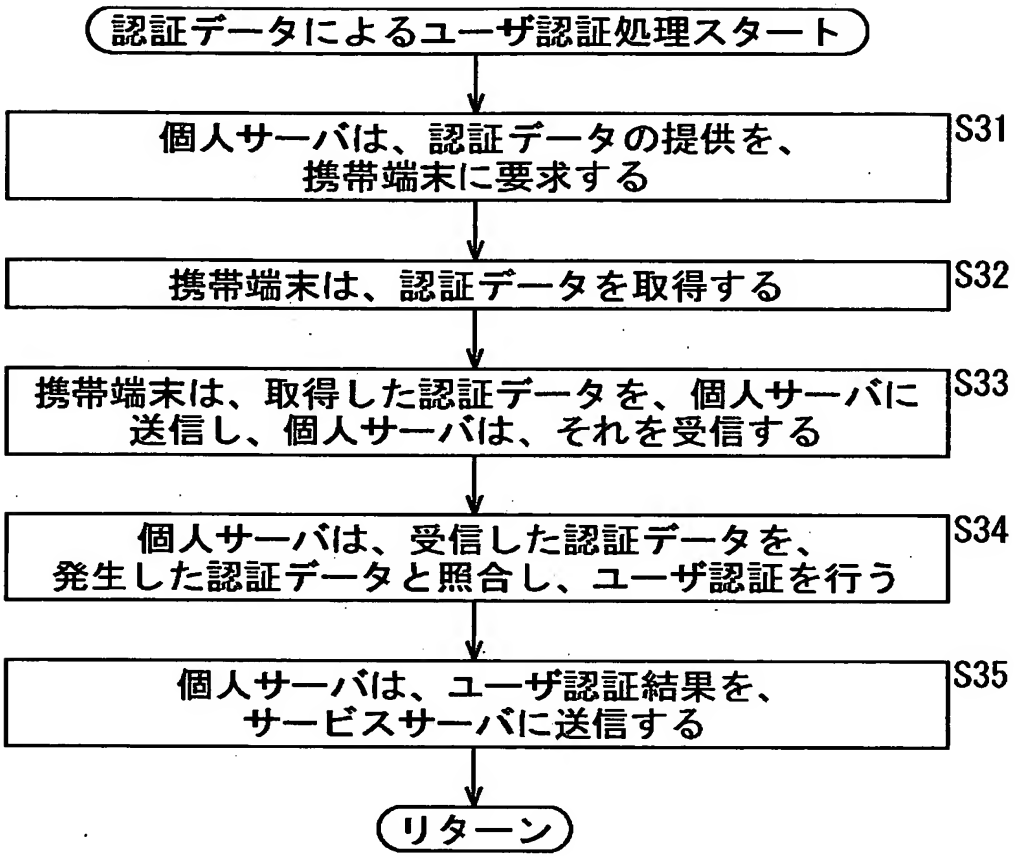
【図６】


精算処理スタート
精算装置は、URL2、購入金額、支払IDを、携帯端末に送信し、携帯端末は、それを受信する
S1
携帯端末は、個人サーバに、URL2、支払ID、購入金額を送信するとともに、サービスサーバとの接続を要求する
S2
個人サーバとサービスサーバの通信確立
S3
個人サーバは、支払ID、購入金額を、サービスサーバに送信し、サービスサーバはそれを受信する
S4
サービスサーバは、ユーザ認証を、個人サーバに要求する
S5
顔写真によるユーザ認証
S6
認証データによるユーザ認証
S7
支払処理
S8
サービスサーバは、支払IDを精算装置に送信する
S9
精算装置は、支払処理の完了を認識する
S10
エンド

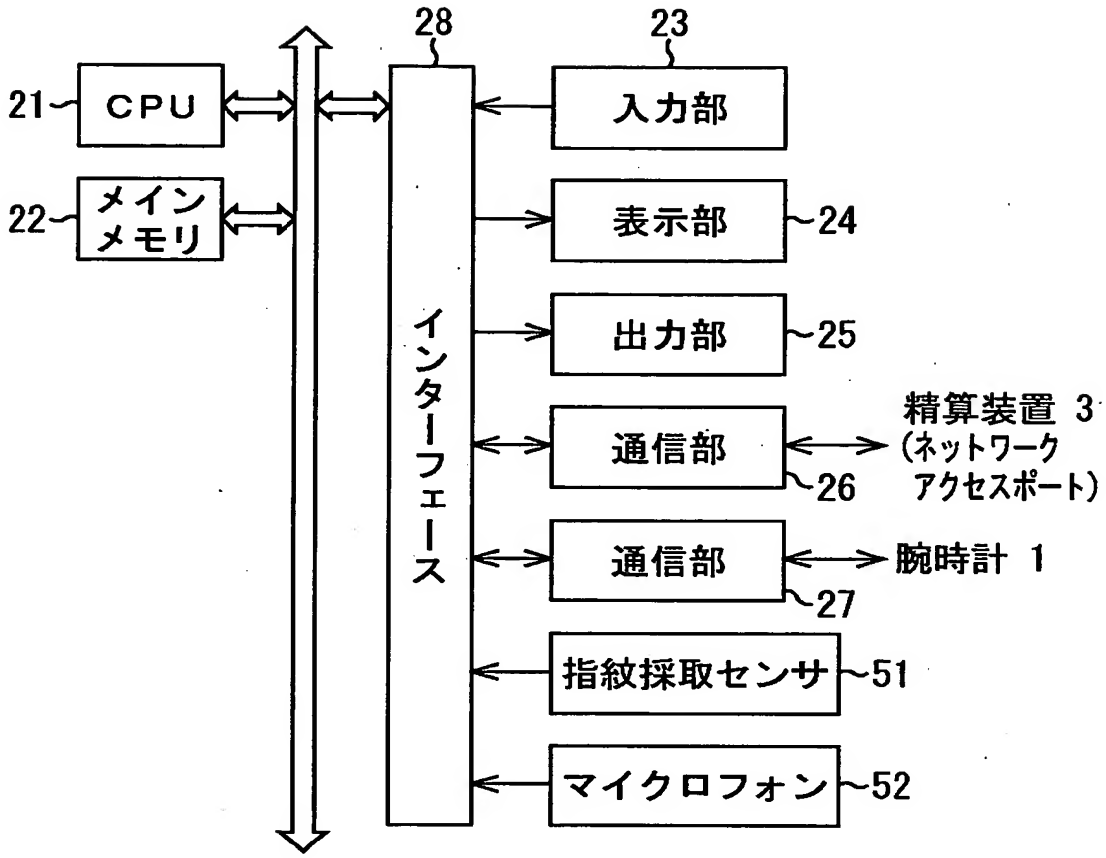
【図７】


顔写真によるユーザ認証処理スタート
個人サーバは、顔写真データを、精算装置に送信し、精算装置は、それを受信する
S21
精算装置は、顔写真データに対応する画像を表示する
S22
精算装置はユーザ認証結果を認識する
S23
精算装置は、認識結果を、個人サーバとサービスサーバに送信する
S24
リターン

【図８】

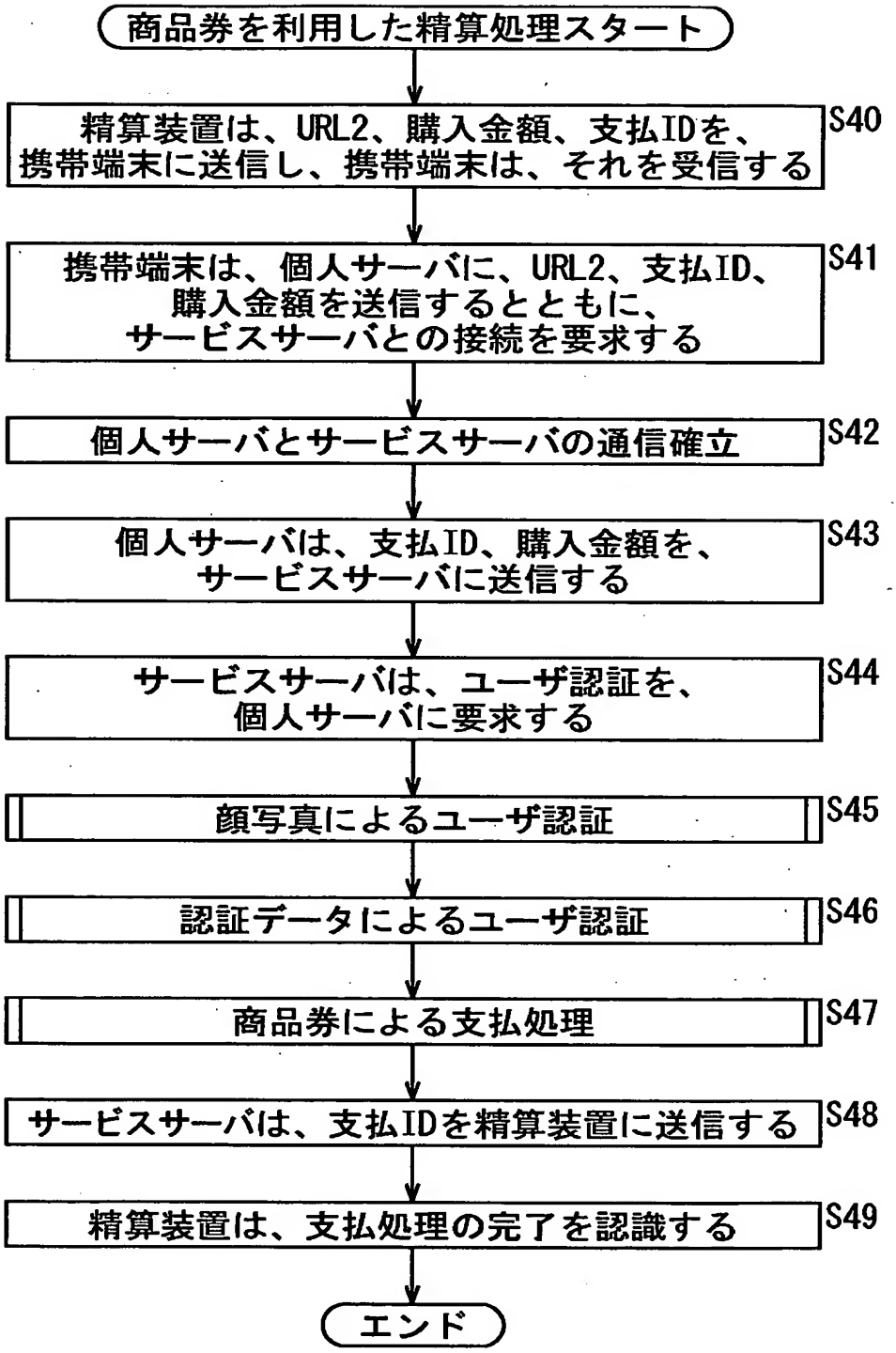

認証データによるユーザ認証処理スタート
個人サーバは、認証データの提供を、携帯端末に要求する
S31
携帯端末は、認証データを取得する
S32
携帯端末は、取得した認証データを、個人サーバに送信し、個人サーバは、それを受信する
S33
個人サーバは、受信した認証データを、発生した認証データと照合し、ユーザ認証を行う
S34
個人サーバは、ユーザ認証結果を、サービスサーバに送信する
S35
リターン

【図９】

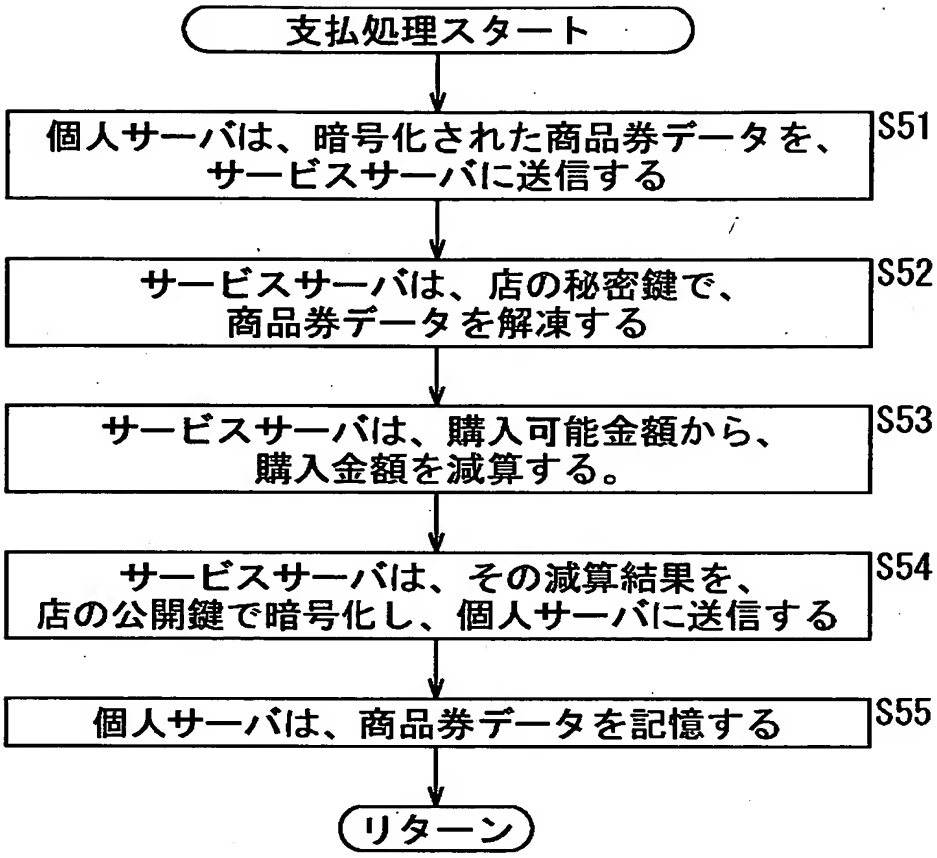

28
23
21
CPU
入力部
22
メイン
メモリ
表示部
24
出力部
25
インターフェース
精算装置 3
(ネットワーク
アクセスポート)
通信部
26
通信部
腕時計 1
27
指紋採取センサ
51
マイクロフォン
52

携帯端末 2

【図１０】

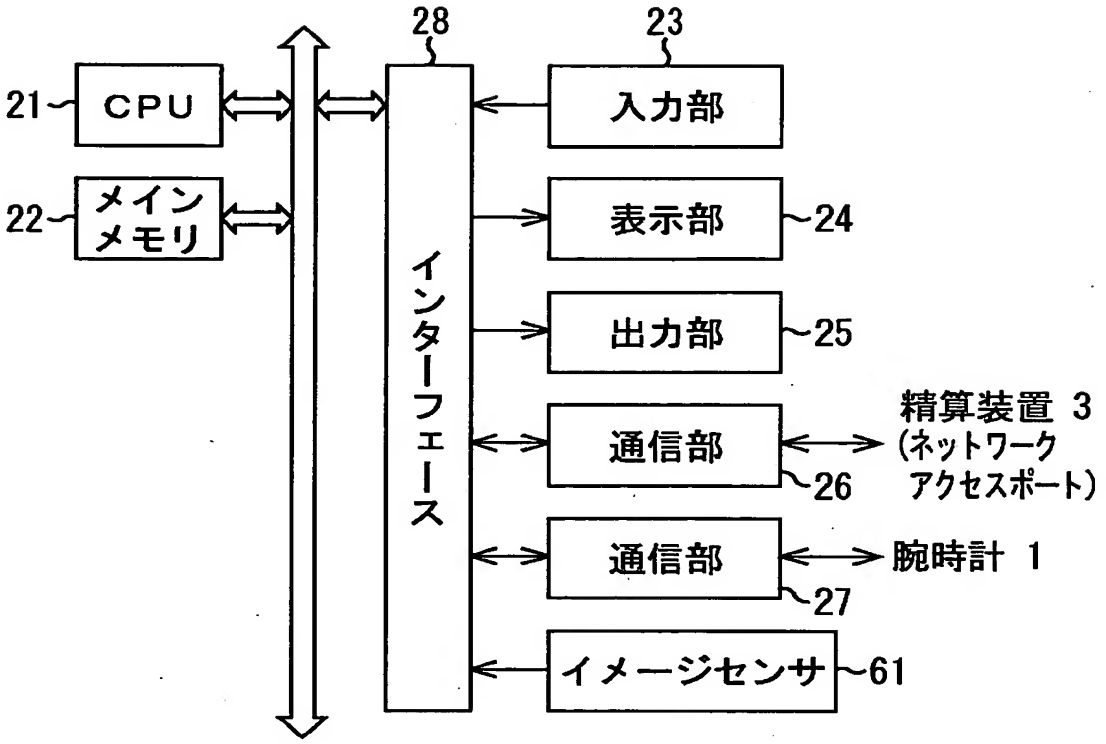

商品券を利用した精算処理スタート
精算装置は、URL2、購入金額、支払IDを、携帯端末に送信し、携帯端末は、それを受信する
S40
携帯端末は、個人サーバに、URL2、支払ID、購入金額を送信するとともに、サービスサーバとの接続を要求する
S41
個人サーバとサービスサーバの通信確立
S42
個人サーバは、支払ID、購入金額を、サービスサーバに送信する
S43
サービスサーバは、ユーザ認証を、個人サーバに要求する
S44
顔写真によるユーザ認証
S45
認証データによるユーザ認証
S46
商品券による支払処理
S47
サービスサーバは、支払IDを精算装置に送信する
S48
精算装置は、支払処理の完了を認識する
S49
エンド

【図１１】



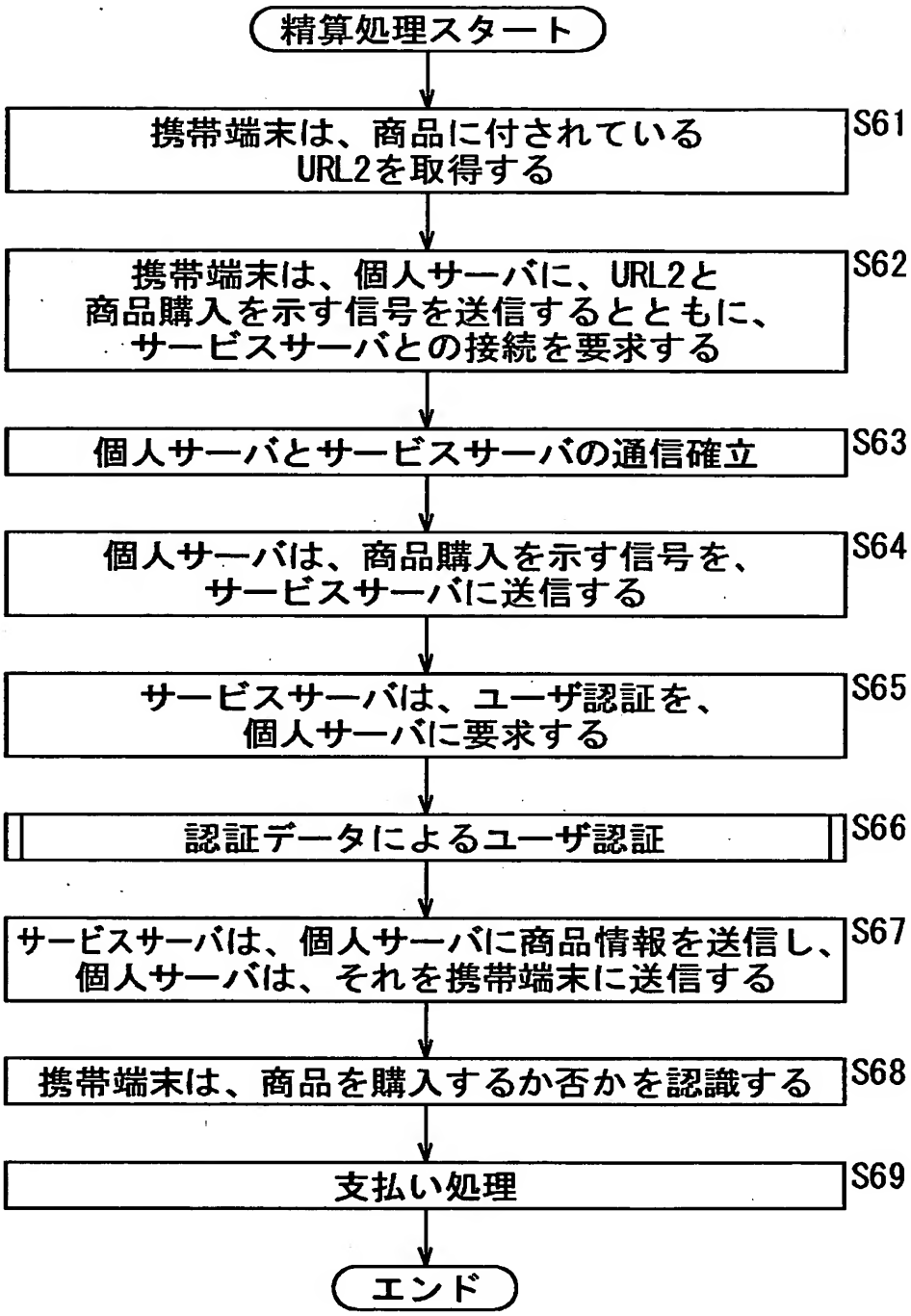
出証特２００１－３０９４８９９

【図１２】

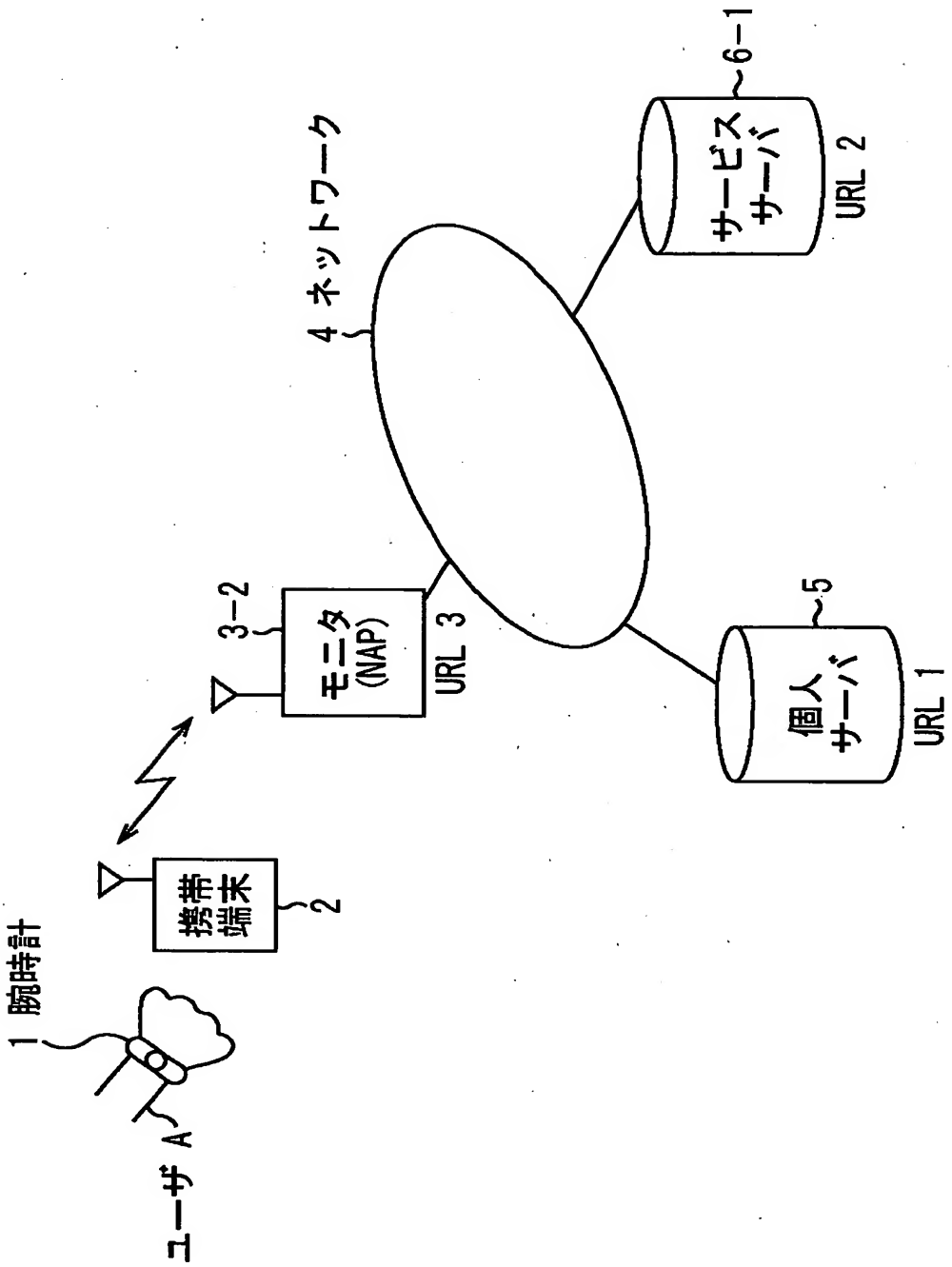

28
23
21
CPU
入力部
22
メイン
メモリ
表示部
24
インターフェース
出力部
25
精算装置 3
(ネットワーク
アクセスポート)
通信部
26
通信部
腕時計 1
27
イメージセンサ
61

携帯端末 2

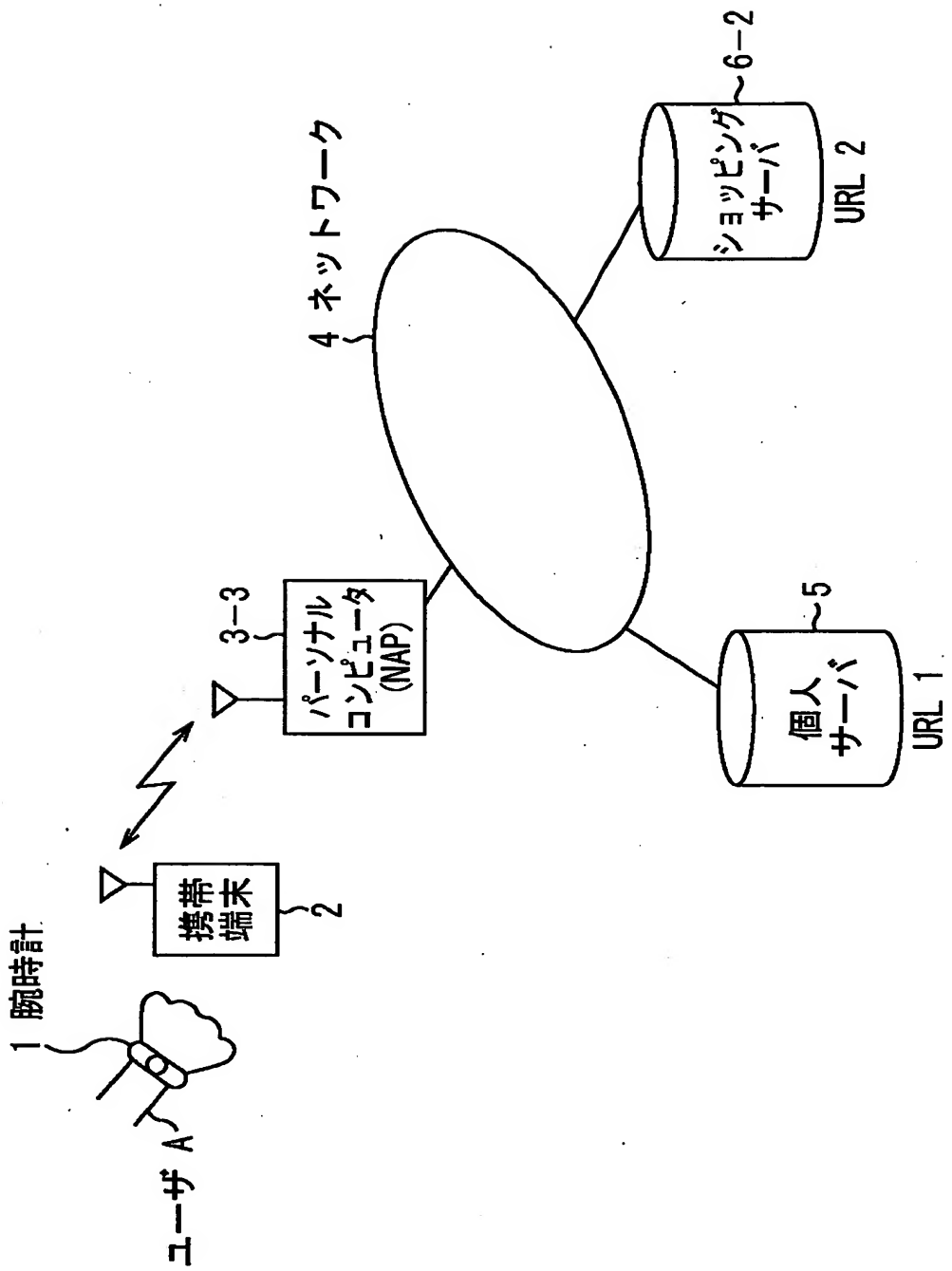
【図１３】


精算処理スタート
携帯端末は、商品に付されている URL2を取得する
S61
携帯端末は、個人サーバに、URL2と 商品購入を示す信号を送信するとともに、 サービスサーバとの接続を要求する
S62
個人サーバとサービスサーバの通信確立
S63
個人サーバは、商品購入を示す信号を、 サービスサーバに送信する
S64
サービスサーバは、ユーザ認証を、 個人サーバに要求する
S65
認証データによるユーザ認証
S66
サービスサーバは、個人サーバに商品情報を送信し、 個人サーバは、それを携帯端末に送信する
S67
携帯端末は、商品を購入するか否かを認識する
S68
支払い処理
S69
エンド

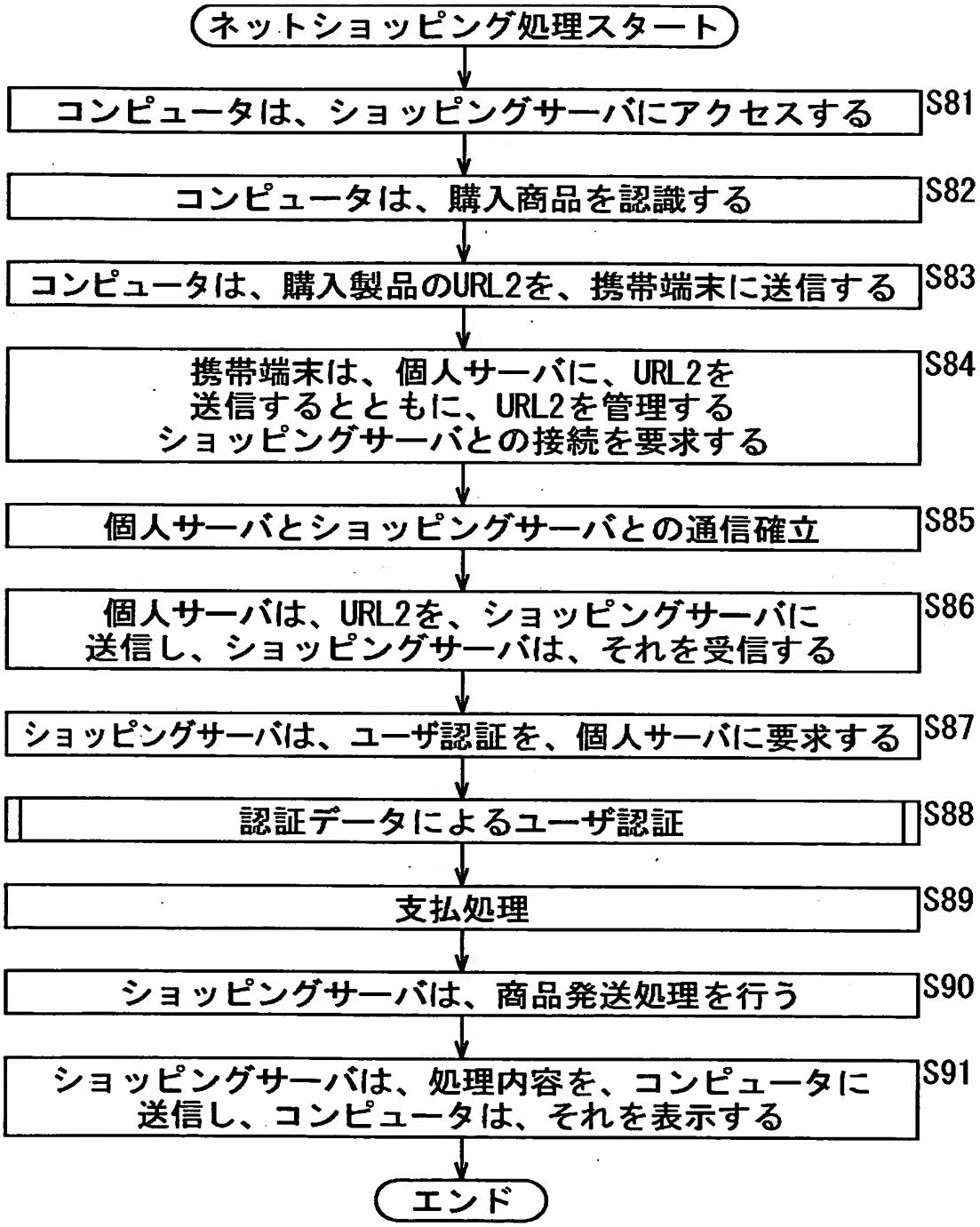
【図１４】


1 腕時計
ユーザ A
携帯端末
2
3-2
モニタ (NAP)
URL 3
4 ネットワーク
5
個人サーバ
URL 1
6-1
サービスサーバ
URL 2

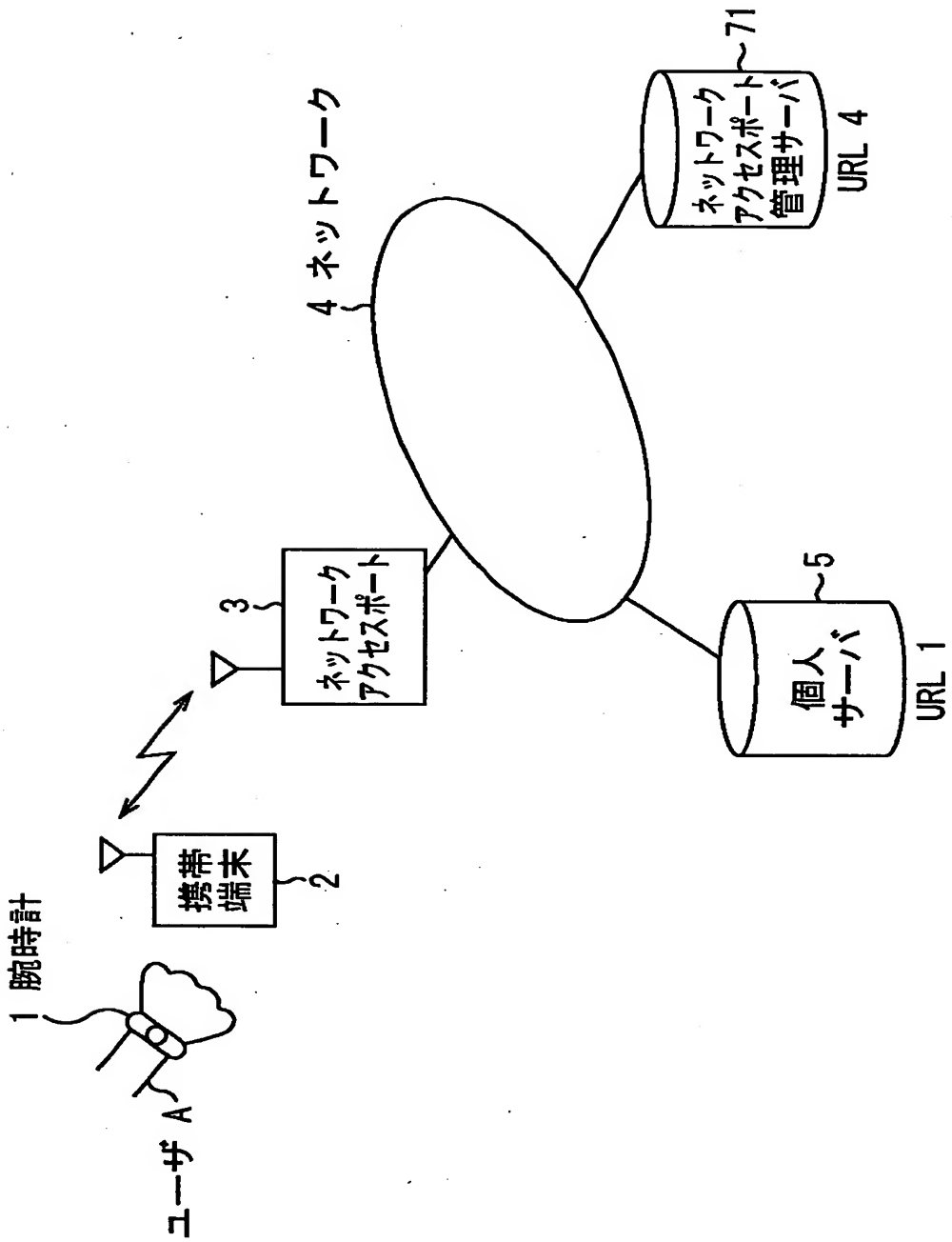
【図１５】


1 腕時計
ユーザ A
2
携帯端末
3-3
パーソナルコンピュータ (NAP)
4 ネットワーク
5
個人サーバ
URL 1
6-2
ショッピングサーバ
URL 2

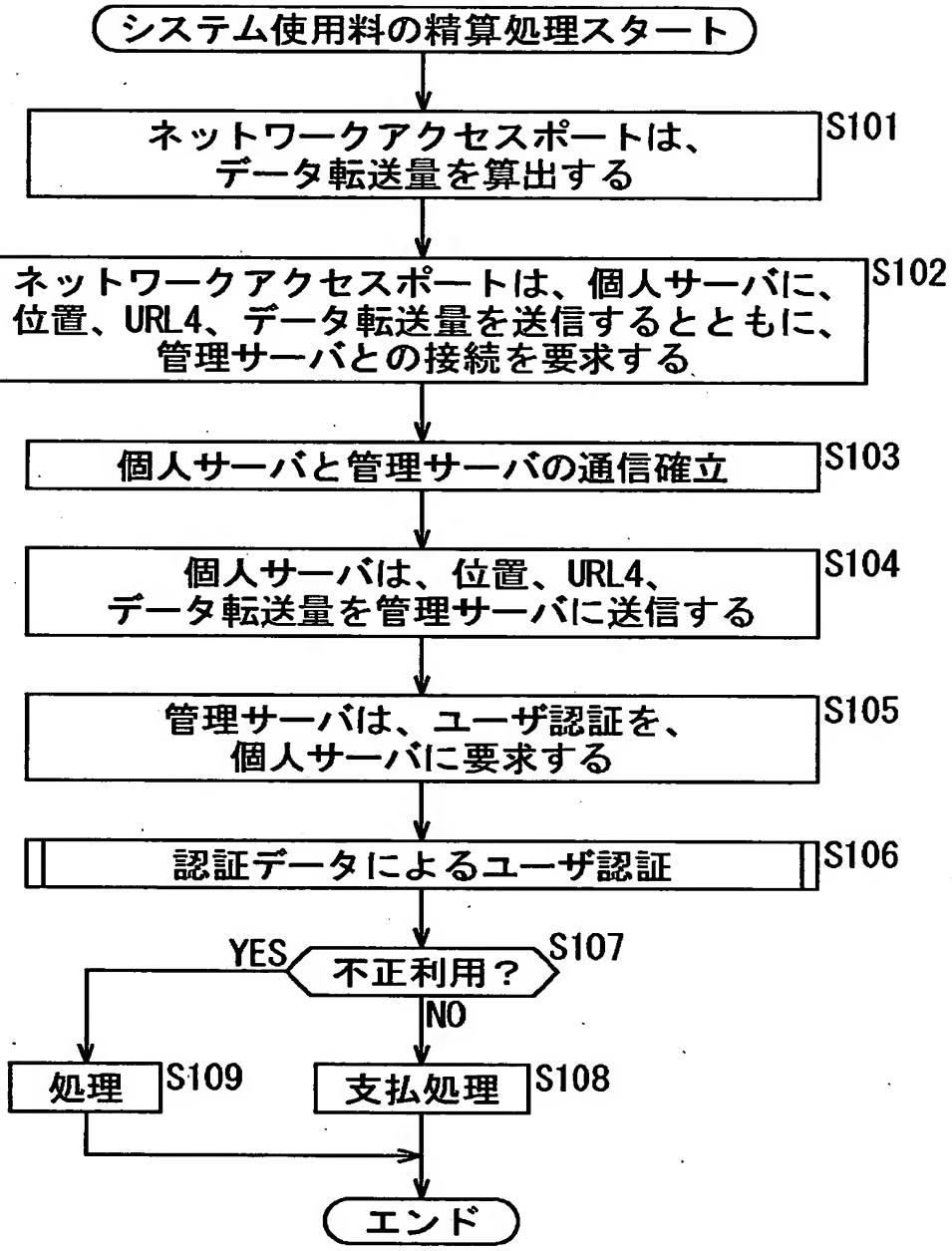
【図１６】


ネットショッピング処理スタート
コンピュータは、ショッピングサーバにアクセスする
S81
コンピュータは、購入商品を認識する
S82
コンピュータは、購入製品のURL2を、携帯端末に送信する
S83
携帯端末は、個人サーバに、URL2を
送信するとともに、URL2を管理する
ショッピングサーバとの接続を要求する
S84
個人サーバとショッピングサーバとの通信確立
S85
個人サーバは、URL2を、ショッピングサーバに
送信し、ショッピングサーバは、それを受信する
S86
ショッピングサーバは、ユーザ認証を、個人サーバに要求する
S87
認証データによるユーザ認証
S88
支払処理
S89
ショッピングサーバは、商品発送処理を行う
S90
ショッピングサーバは、処理内容を、コンピュータに
送信し、コンピュータは、それを表示する
S91
エンド

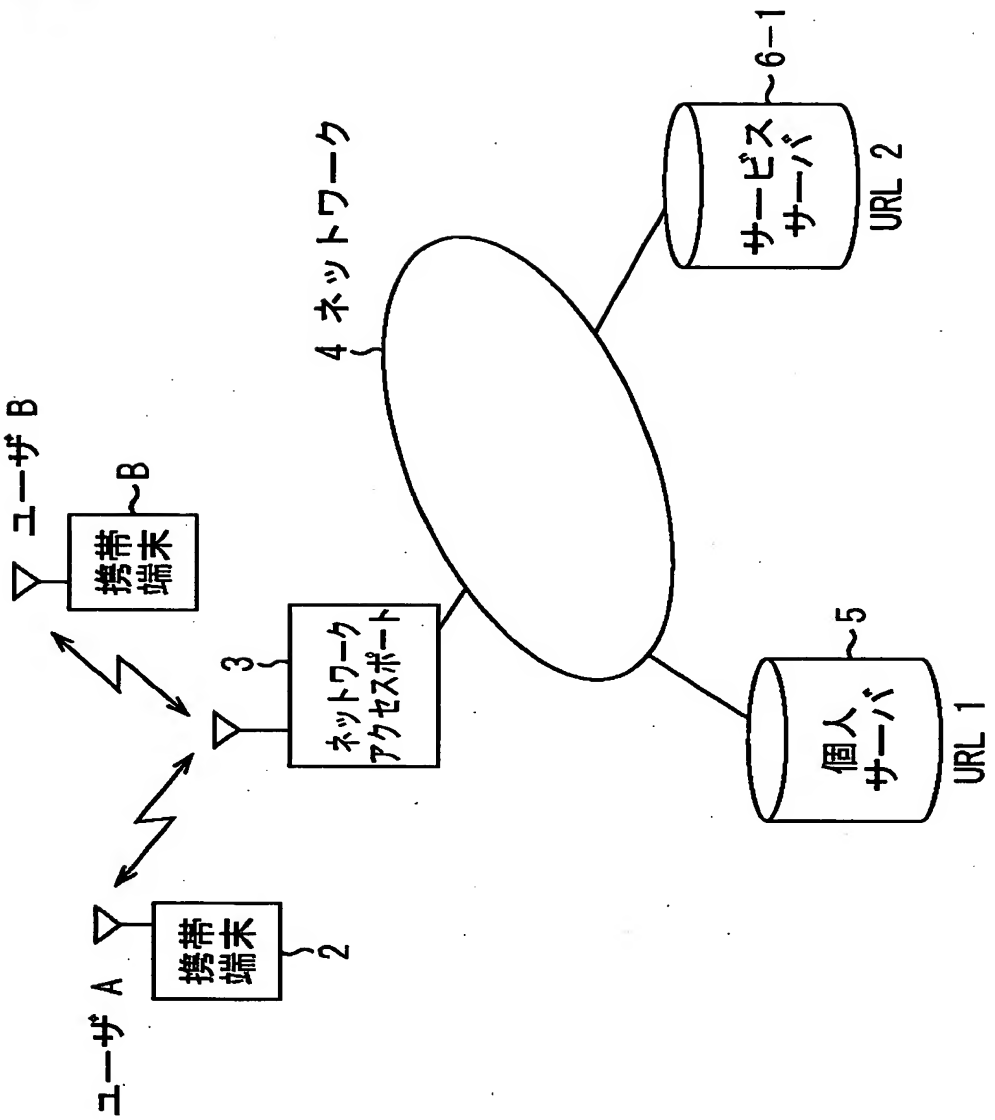
【図１７】


1 腕時計
ユーザ A
2
携帯端末
3
ネットワーク
アクセスポート
4 ネットワーク
71
ネットワーク
アクセスポート
管理サーバ
URL 4
5
個人
サーバ
URL 1

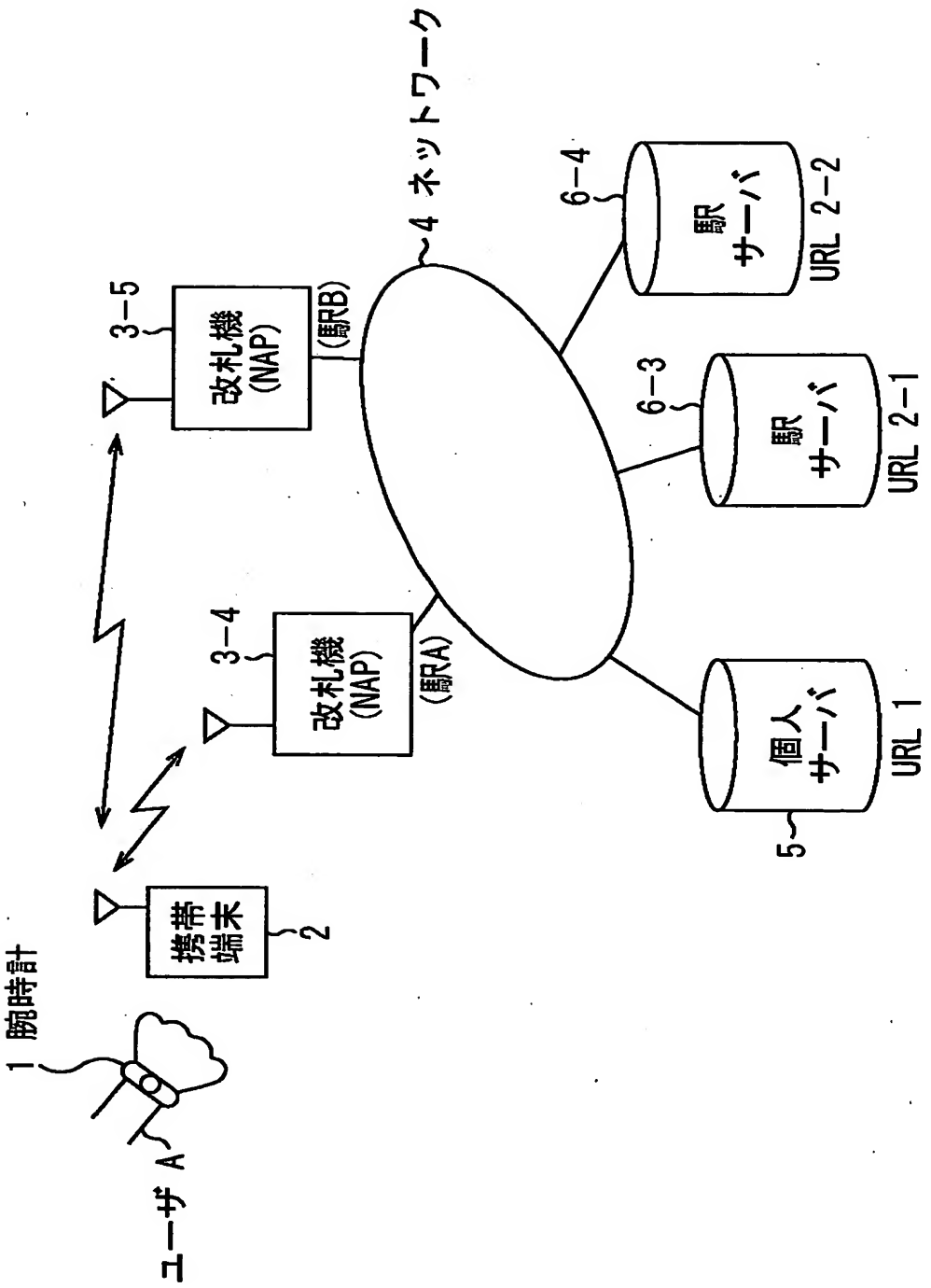
【図１８】


システム使用料の精算処理スタート
ネットワークアクセスポートは、
データ転送量を算出する
S101
ネットワークアクセスポートは、個人サーバに、
位置、URL4、データ転送量を送信するとともに、
管理サーバとの接続を要求する
S102
個人サーバと管理サーバの通信確立
S103
個人サーバは、位置、URL4、
データ転送量を管理サーバに送信する
S104
管理サーバは、ユーザ認証を、
個人サーバに要求する
S105
認証データによるユーザ認証
S106
YES
不正利用？
S107
NO
処理
S109
支払処理
S108
エンド

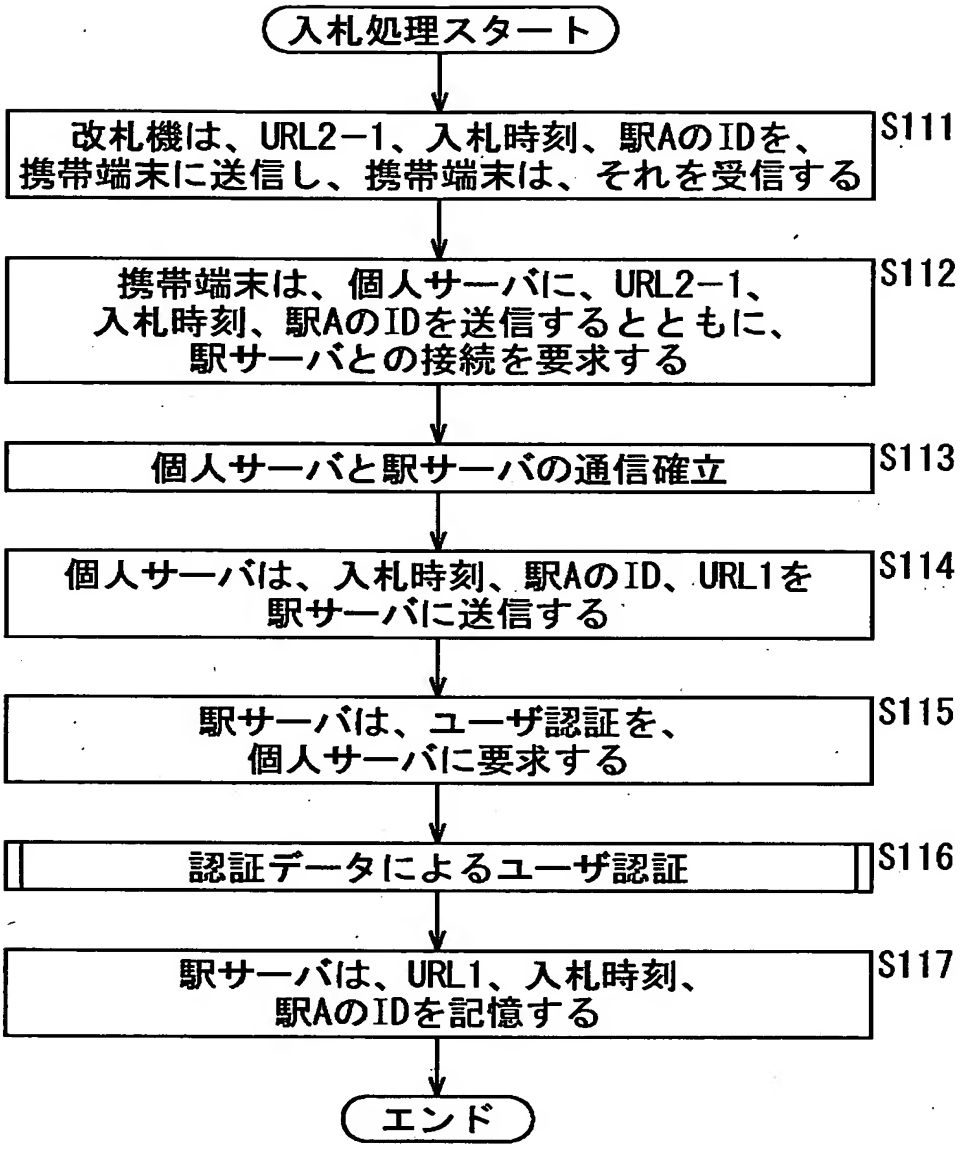
【図１９】


ユーザ A
携帯端末
2
ユーザ B
携帯端末
B
3
ネットワークアクセスポート
4 ネットワーク
5
個人サーバ
URL 1
6-1
サービスサーバ
URL 2

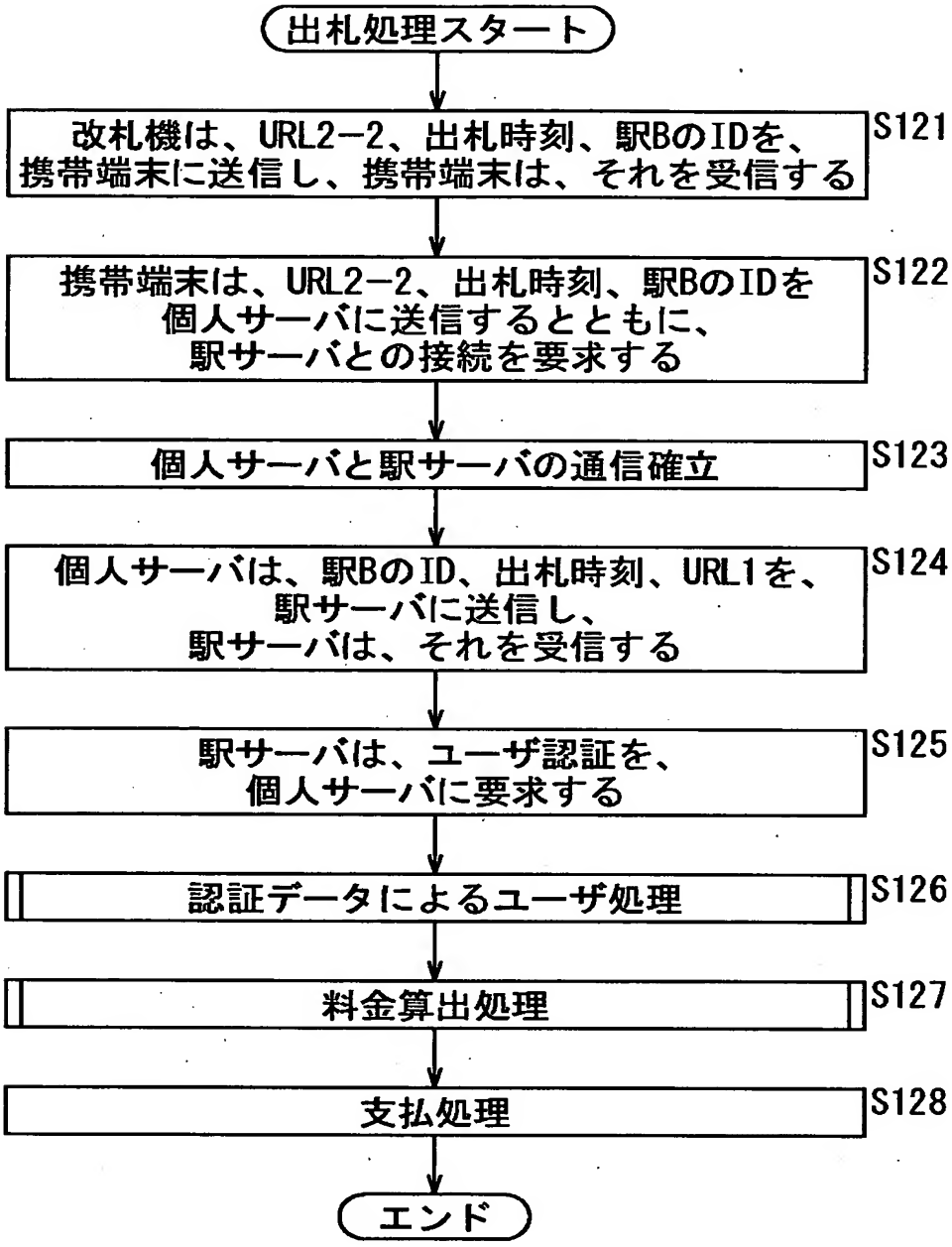
【図２０】


1 腕時計
ユーザ A
2
携帯端末
3-4
改札機 (NAP)
(駅A)
3-5
改札機 (NAP)
(駅B)
4 ネットワーク
5
個人サーバ
URL 1
6-3
駅サーバ
URL 2-1
6-4
駅サーバ
URL 2-2

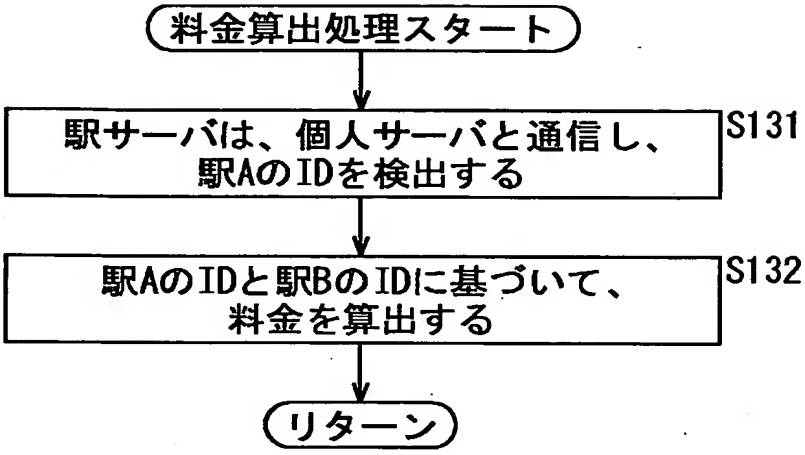
【図２１】


入札処理スタート
改札機は、URL2−1、入札時刻、駅AのIDを、携帯端末に送信し、携帯端末は、それを受信する
S111
携帯端末は、個人サーバに、URL2−1、入札時刻、駅AのIDを送信するとともに、駅サーバとの接続を要求する
S112
個人サーバと駅サーバの通信確立
S113
個人サーバは、入札時刻、駅AのID、URL1を駅サーバに送信する
S114
駅サーバは、ユーザ認証を、個人サーバに要求する
S115
認証データによるユーザ認証
S116
駅サーバは、URL1、入札時刻、駅AのIDを記憶する
S117
エンド

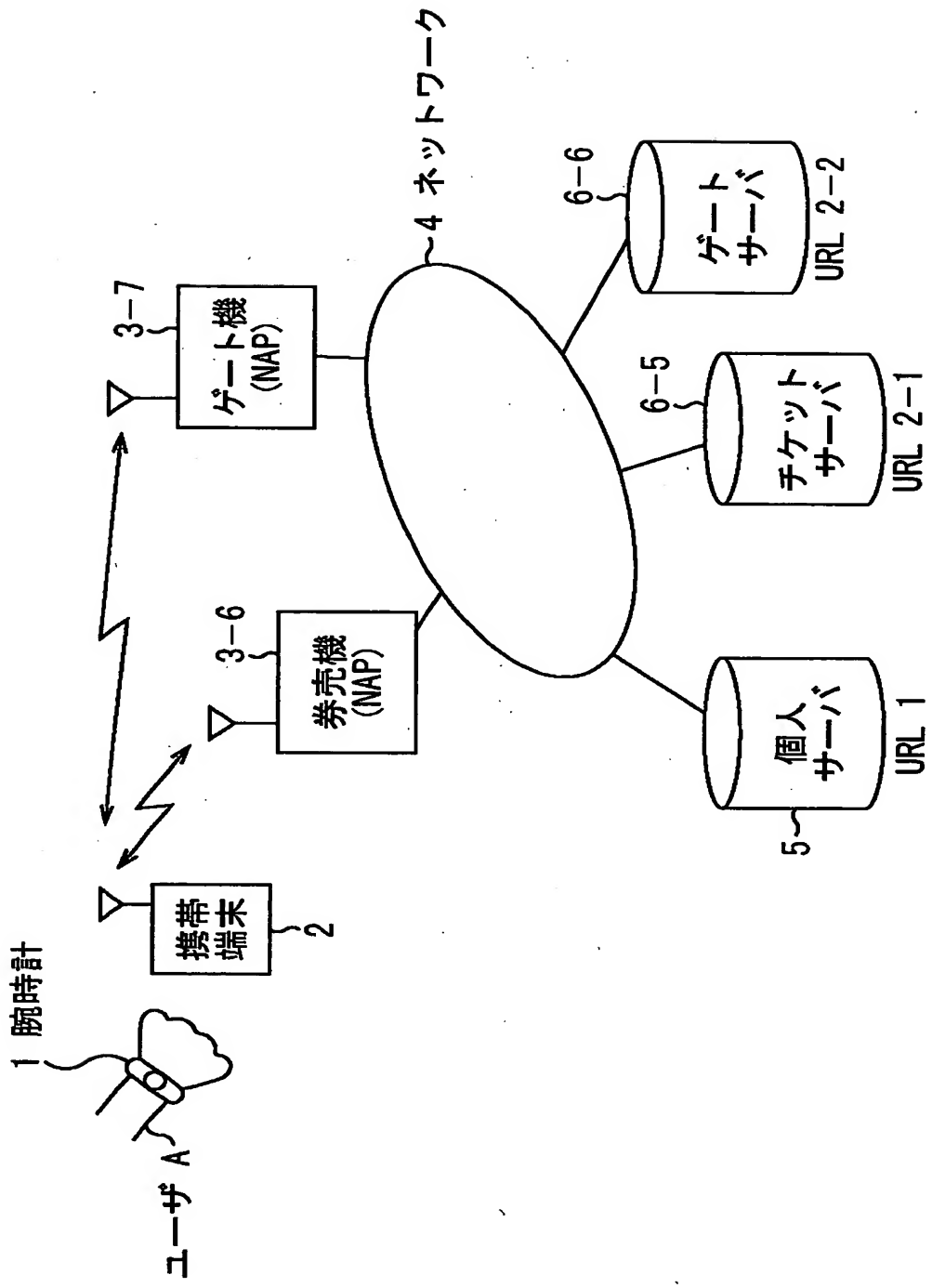
【図２２】


出札処理スタート
改札機は、URL2−2、出札時刻、駅BのIDを、携帯端末に送信し、携帯端末は、それを受信する
S121
携帯端末は、URL2−2、出札時刻、駅BのIDを個人サーバに送信するとともに、駅サーバとの接続を要求する
S122
個人サーバと駅サーバの通信確立
S123
個人サーバは、駅BのID、出札時刻、URL1を、駅サーバに送信し、駅サーバは、それを受信する
S124
駅サーバは、ユーザ認証を、個人サーバに要求する
S125
認証データによるユーザ処理
S126
料金算出処理
S127
支払処理
S128
エンド

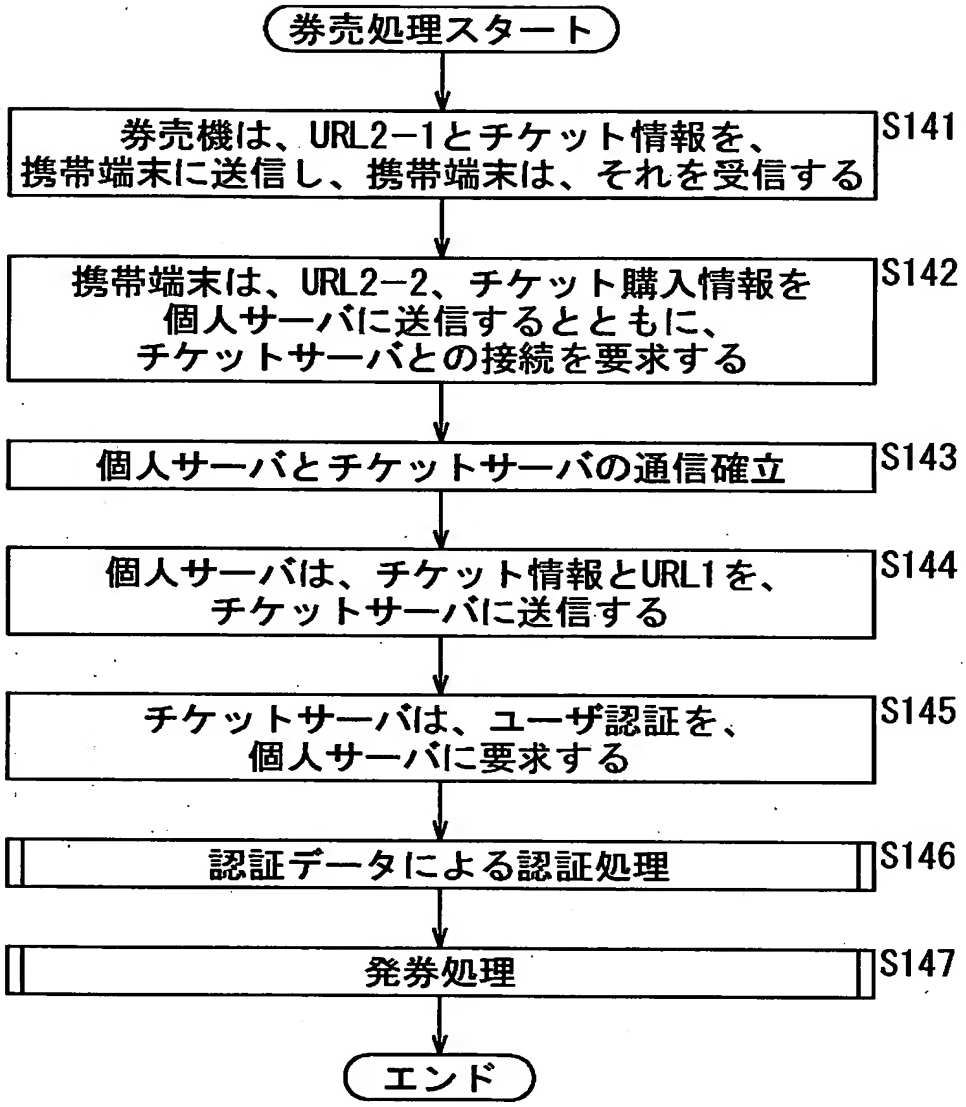
【図２３】


料金算出処理スタート
駅サーバは、個人サーバと通信し、
駅AのIDを検出する
S131
駅AのIDと駅BのIDに基づいて、
料金を算出する
S132
リターン

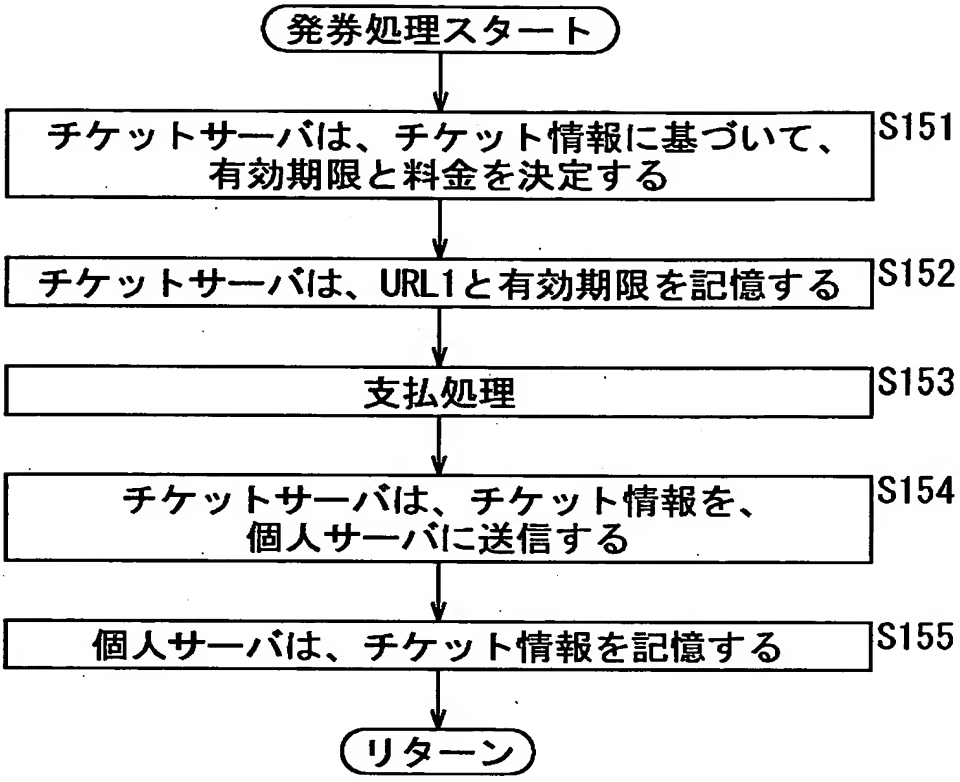
【図２４】


1 腕時計
ユーザ A
2
携帯端末
3-7
ゲート機 (NAP)
3-6
券売機 (NAP)
4 ネットワーク
5
個人サーバ
URL 1
6-5
チケットサーバ
URL 2-1
6-6
ゲートサーバ
URL 2-2

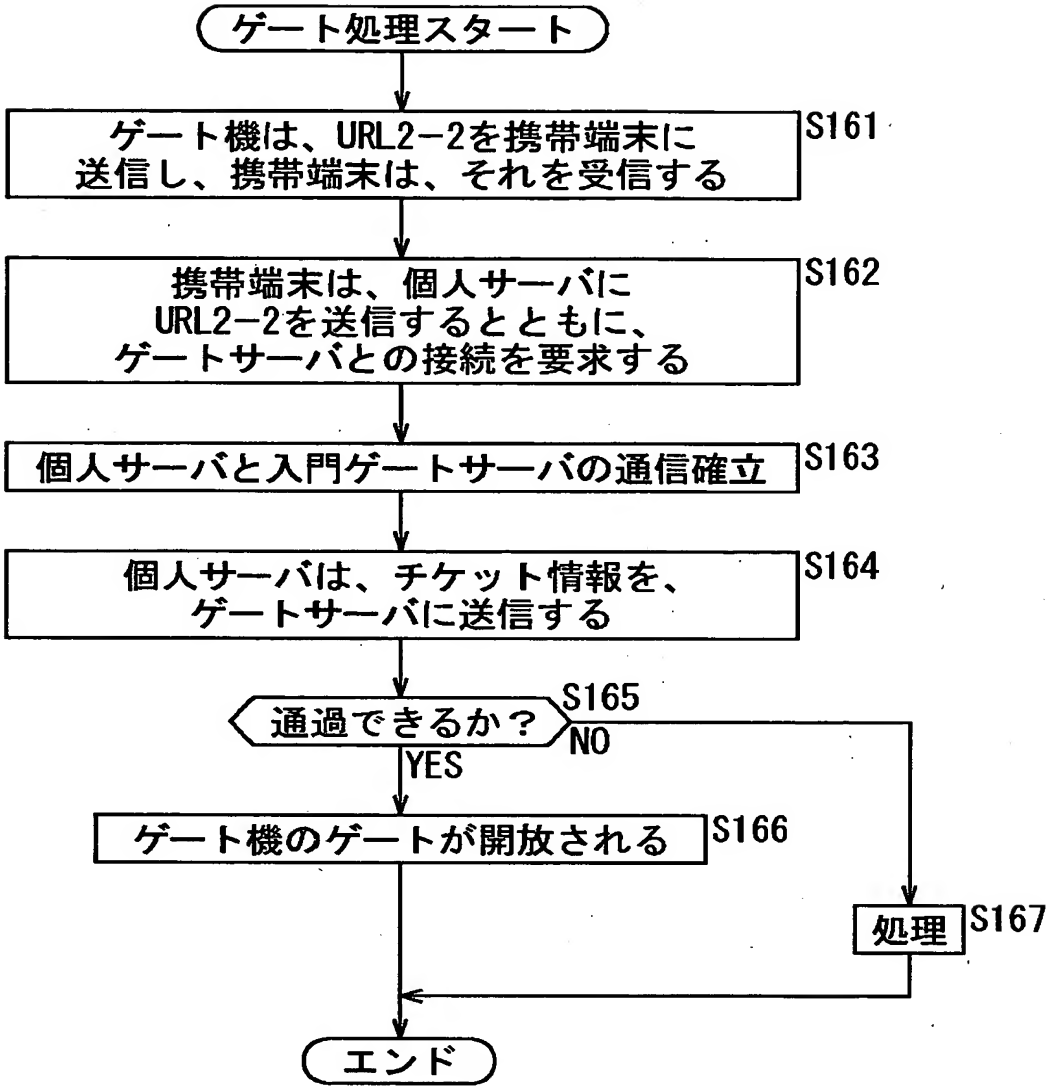
【図２５】


券売処理スタート
券売機は、URL2−1とチケット情報を、携帯端末に送信し、携帯端末は、それを受信する
S141
携帯端末は、URL2−2、チケット購入情報を個人サーバに送信するとともに、チケットサーバとの接続を要求する
S142
個人サーバとチケットサーバの通信確立
S143
個人サーバは、チケット情報とURL1を、チケットサーバに送信する
S144
チケットサーバは、ユーザ認証を、個人サーバに要求する
S145
認証データによる認証処理
S146
発券処理
S147
エンド

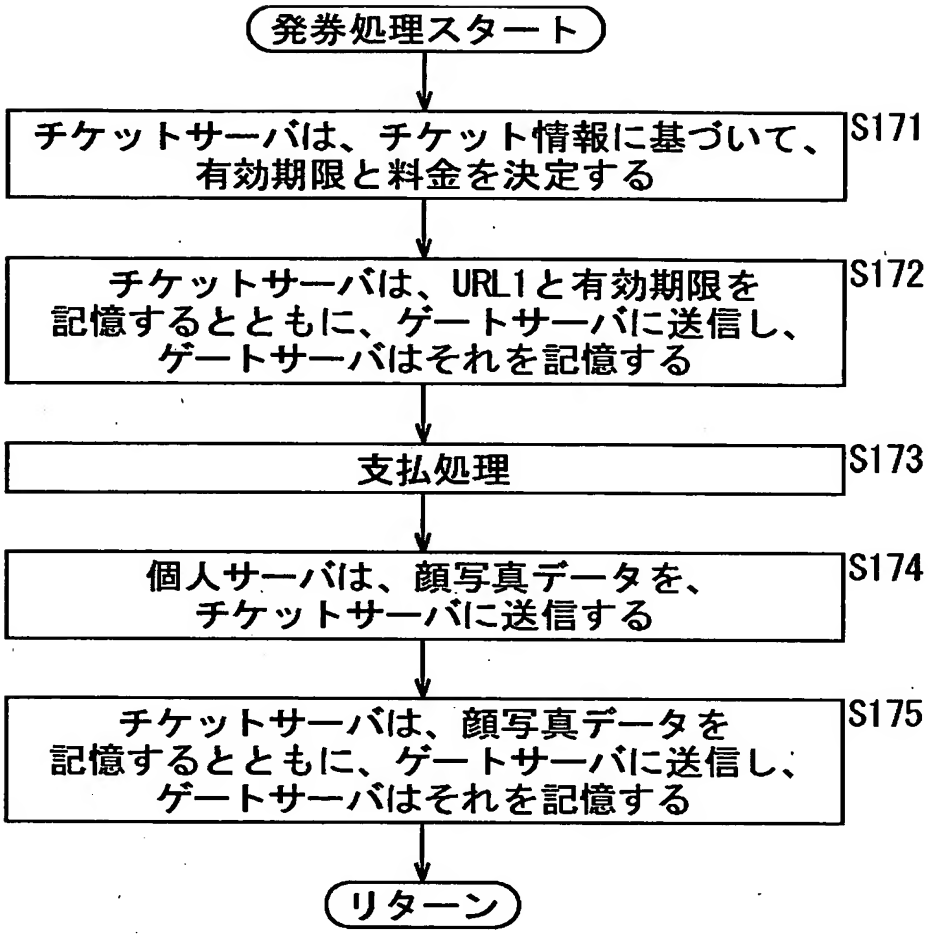
【図２６】


発券処理スタート
チケットサーバは、チケット情報に基づいて、有効期限と料金を決定する
S151
チケットサーバは、URL1と有効期限を記憶する
S152
支払処理
S153
チケットサーバは、チケット情報を、個人サーバに送信する
S154
個人サーバは、チケット情報を記憶する
S155
リターン

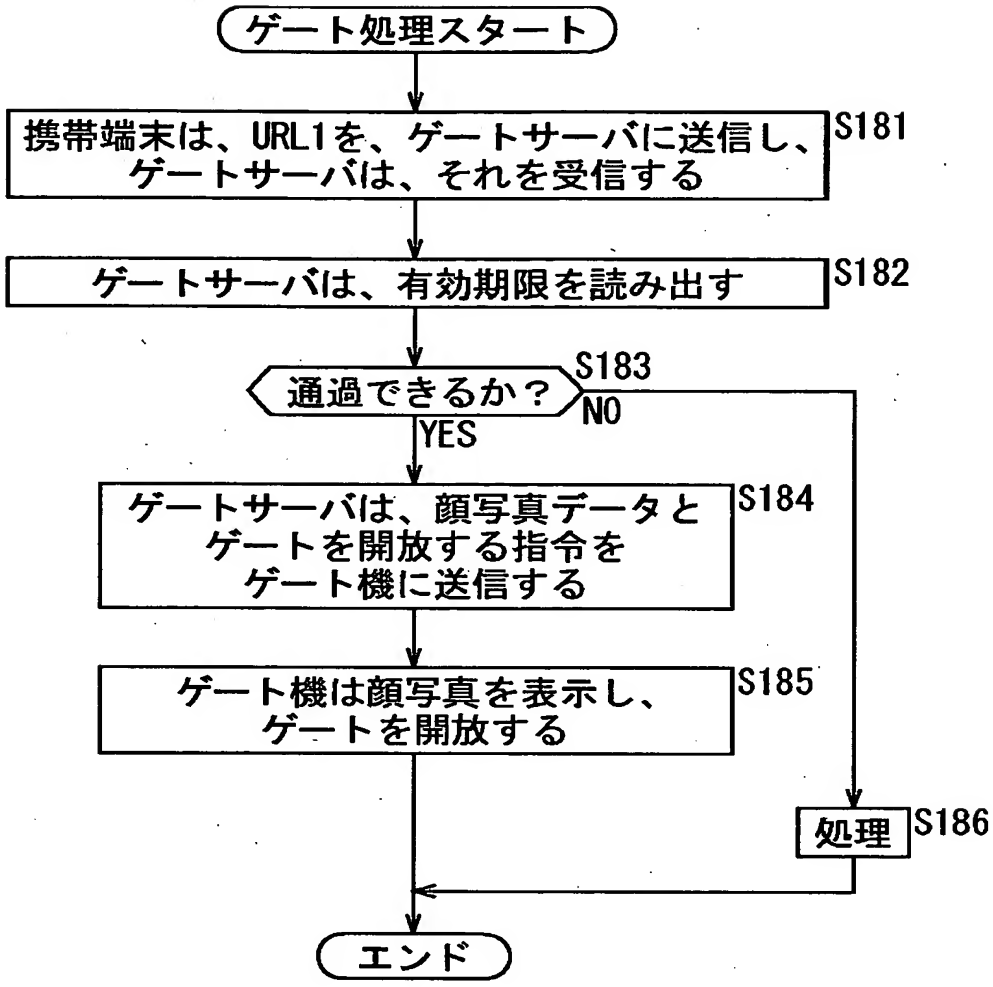
【図２７】


ゲート処理スタート
ゲート機は、URL2−2を携帯端末に送信し、携帯端末は、それを受信する
S161
携帯端末は、個人サーバにURL2−2を送信するとともに、ゲートサーバとの接続を要求する
S162
個人サーバと入門ゲートサーバの通信確立
S163
個人サーバは、チケット情報を、ゲートサーバに送信する
S164
通過できるか？
S165
NO
YES
ゲート機のゲートが開放される
S166
処理
S167
エンド

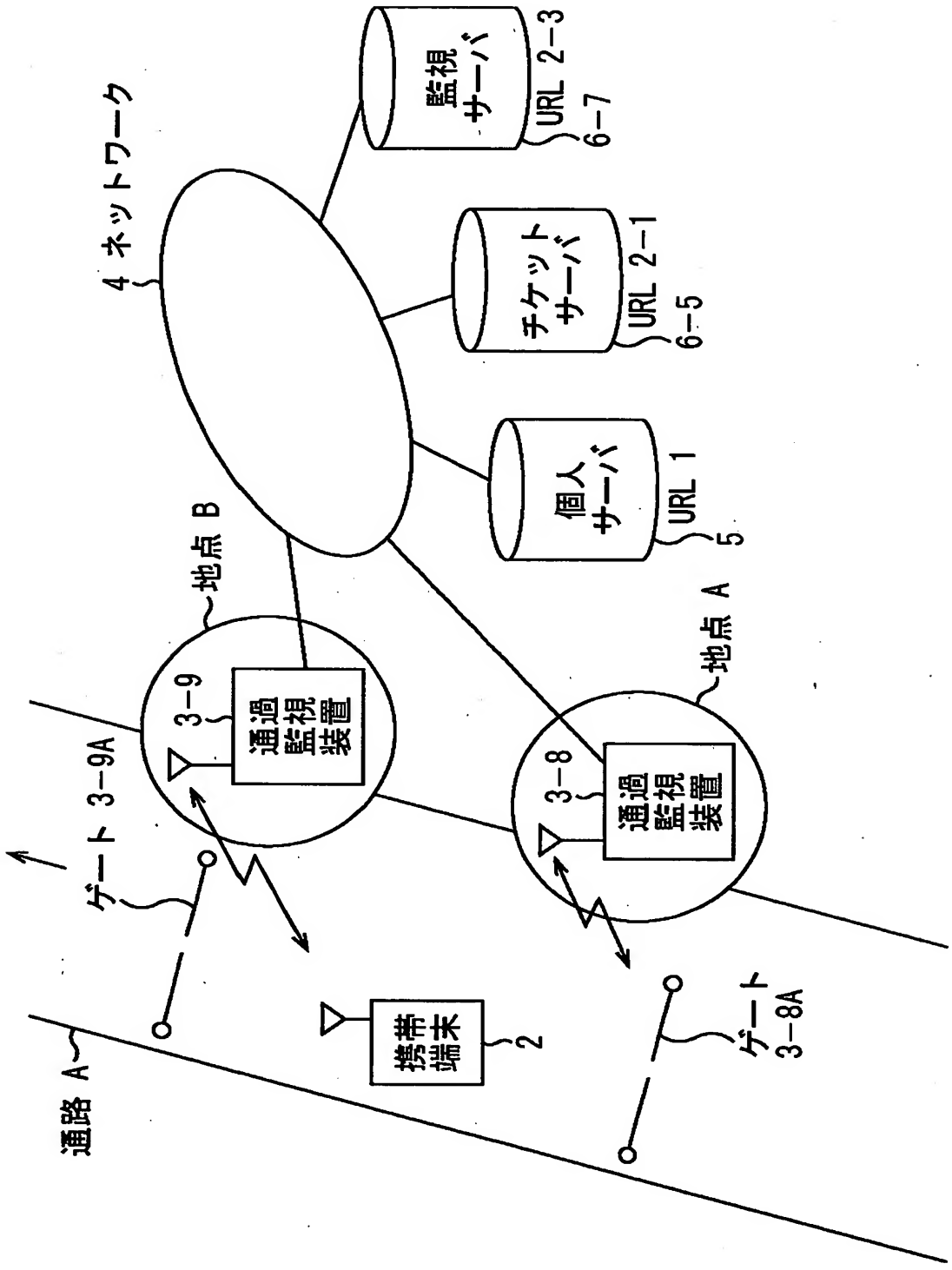
【図２８】


発券処理スタート
チケットサーバは、チケット情報に基づいて、有効期限と料金を決定する
S171
チケットサーバは、URL1と有効期限を記憶するとともに、ゲートサーバに送信し、ゲートサーバはそれを記憶する
S172
支払処理
S173
個人サーバは、顔写真データを、チケットサーバに送信する
S174
チケットサーバは、顔写真データを記憶するとともに、ゲートサーバに送信し、ゲートサーバはそれを記憶する
S175
リターン

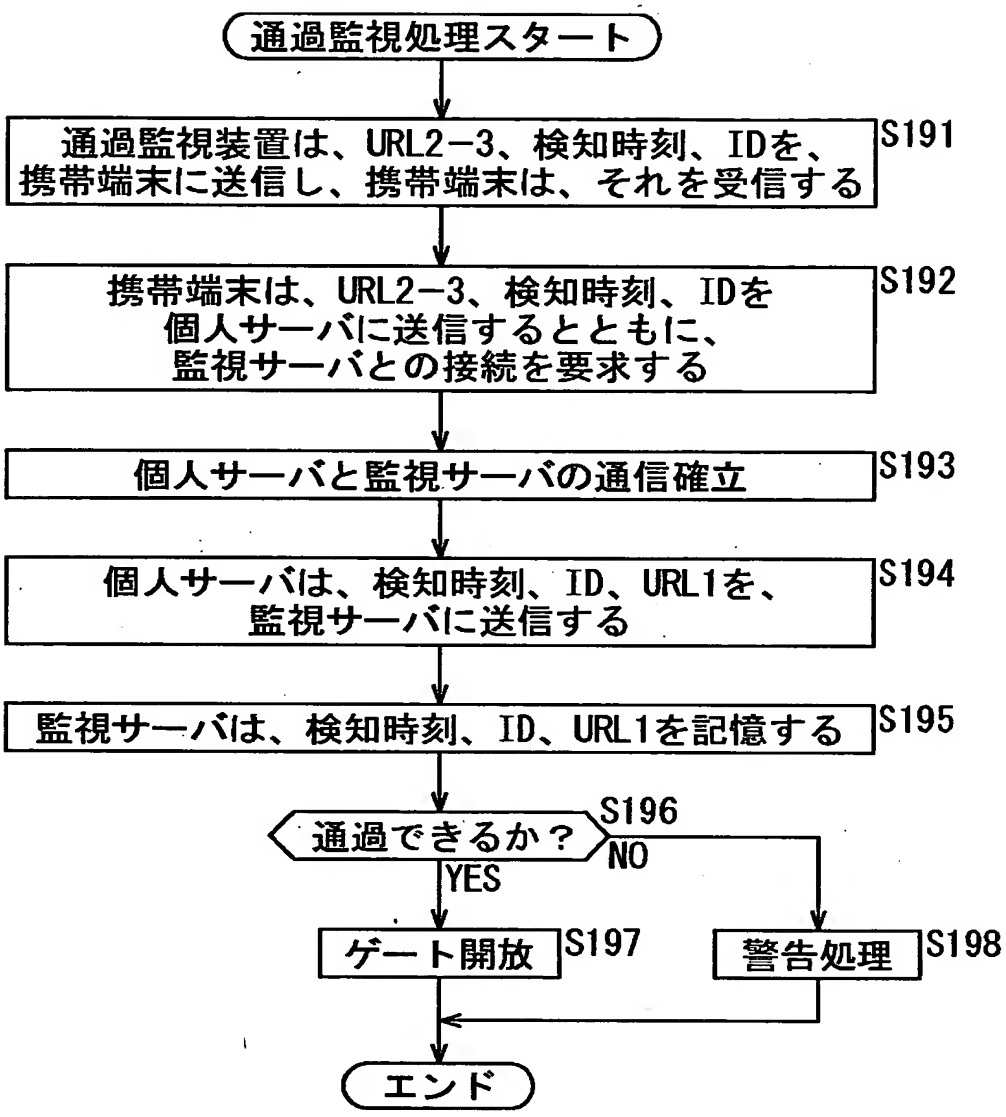
【図２９】


ゲート処理スタート
携帯端末は、URL1を、ゲートサーバに送信し、
ゲートサーバは、それを受信する
S181
ゲートサーバは、有効期限を読み出す
S182
通過できるか？
S183
NO
YES
ゲートサーバは、顔写真データと
ゲートを開放する指令を
ゲート機に送信する
S184
ゲート機は顔写真を表示し、
ゲートを開放する
S185
処理
S186
エンド

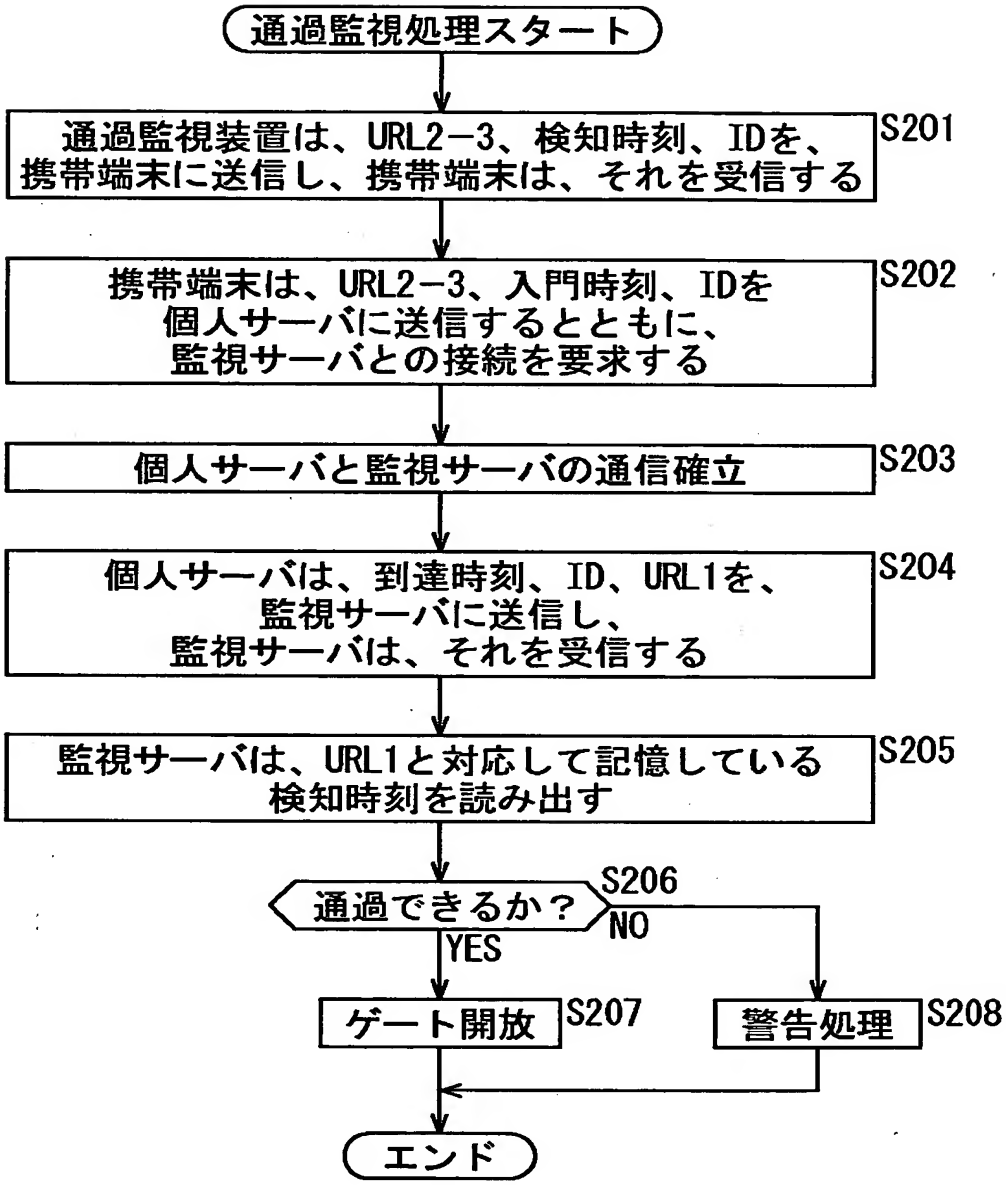
【図３０】


監視サーバ
URL 2-3
6-7
4 ネットワーク
チケットサーバ
URL 2-1
6-5
個人サーバ
URL 1
5
地点 B
地点 A
3-9
通過監視装置
3-8
通過監視装置
ゲート 3-9A
携帯端末
2
ゲート 3-8A
通路 A

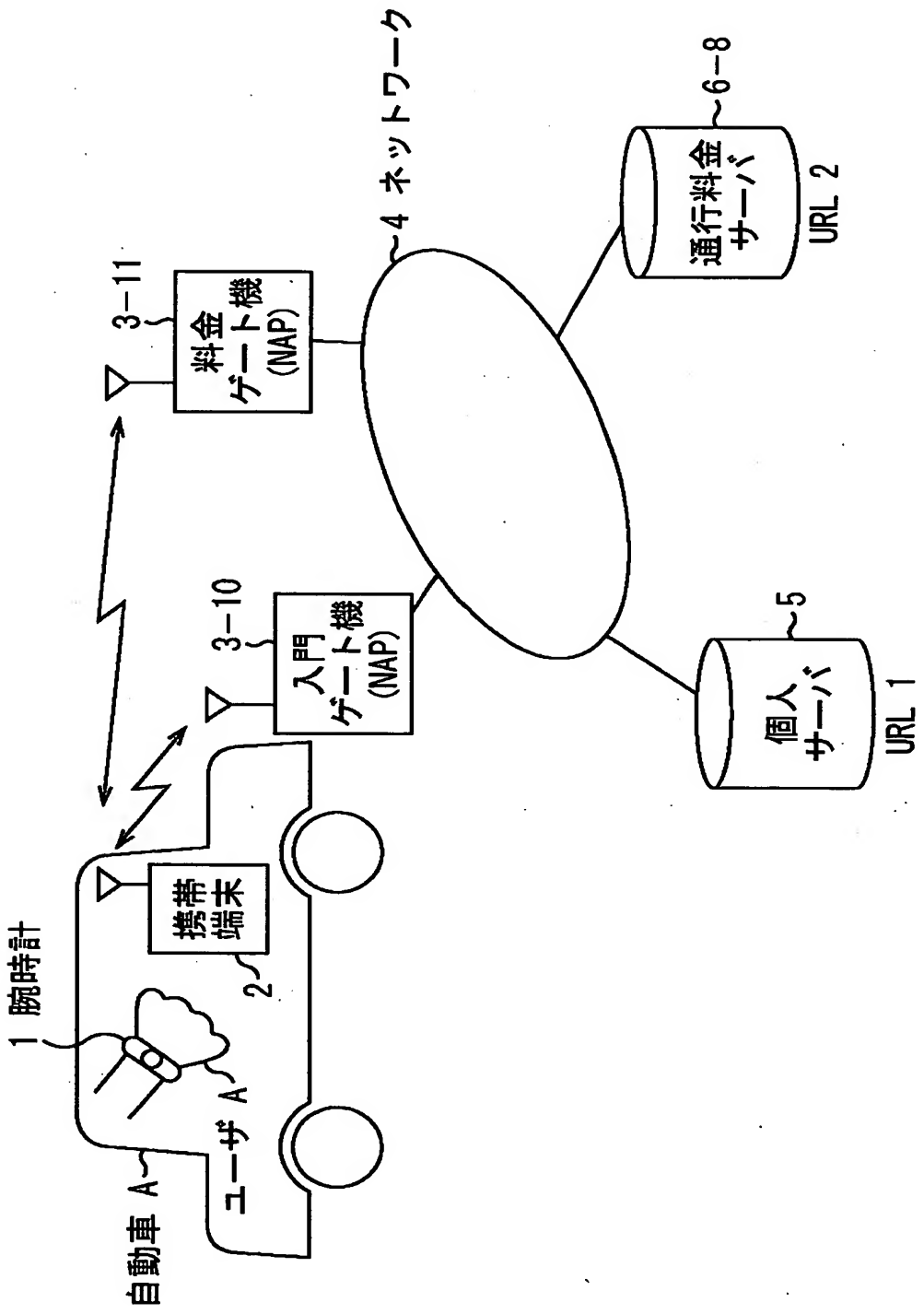
【図３１】


通過監視処理スタート
通過監視装置は、URL2−3、検知時刻、IDを、携帯端末に送信し、携帯端末は、それを受信する
S191
携帯端末は、URL2−3、検知時刻、IDを個人サーバに送信するとともに、監視サーバとの接続を要求する
S192
個人サーバと監視サーバの通信確立
S193
個人サーバは、検知時刻、ID、URL1を、監視サーバに送信する
S194
監視サーバは、検知時刻、ID、URL1を記憶する
S195
通過できるか？
S196
NO
YES
ゲート開放
S197
警告処理
S198
エンド

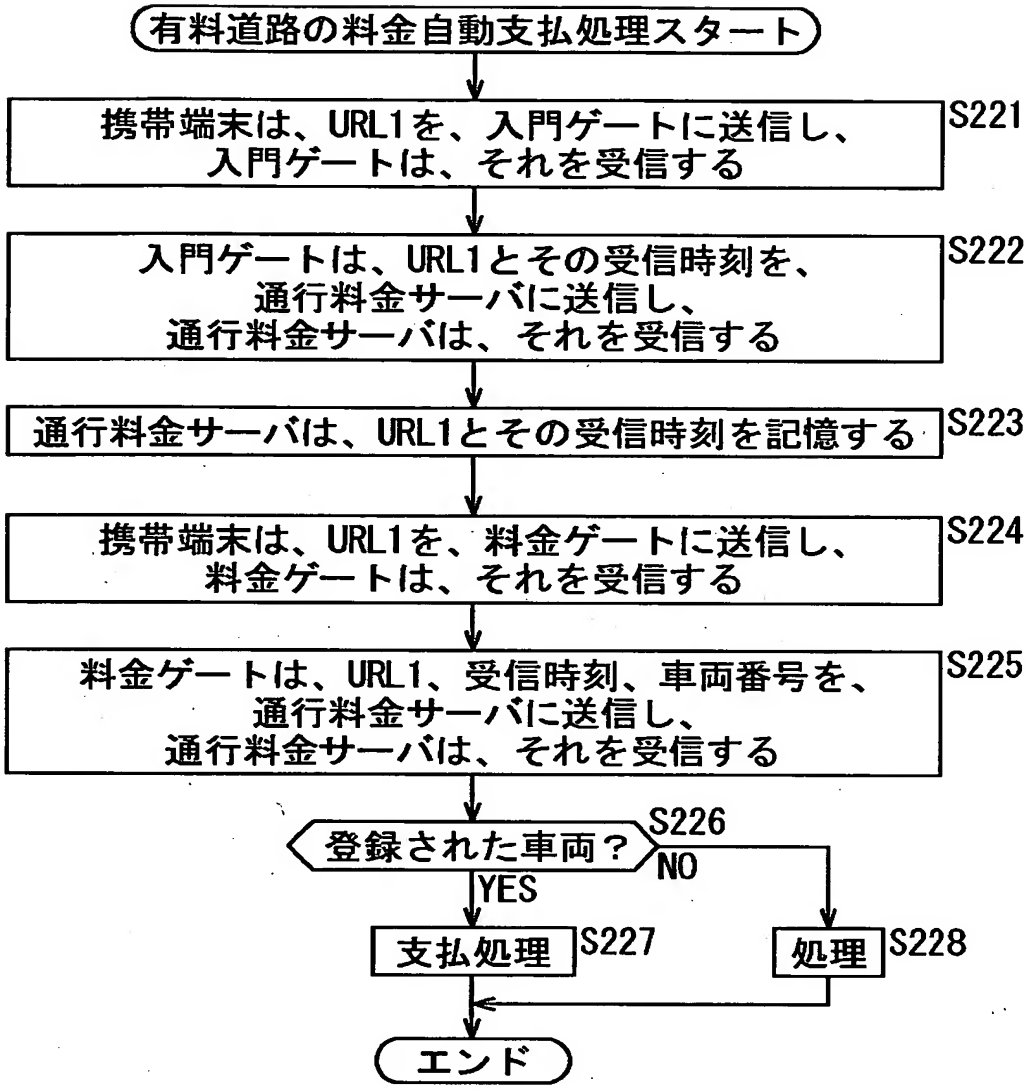
【図３２】


通過監視処理スタート
通過監視装置は、URL2−3、検知時刻、IDを、携帯端末に送信し、携帯端末は、それを受信する
S201
携帯端末は、URL2−3、入門時刻、IDを個人サーバに送信するとともに、監視サーバとの接続を要求する
S202
個人サーバと監視サーバの通信確立
S203
個人サーバは、到達時刻、ID、URL1を、監視サーバに送信し、監視サーバは、それを受信する
S204
監視サーバは、URL1と対応して記憶している検知時刻を読み出す
S205
通過できるか？
S206
NO
YES
ゲート開放
S207
警告処理
S208
エンド

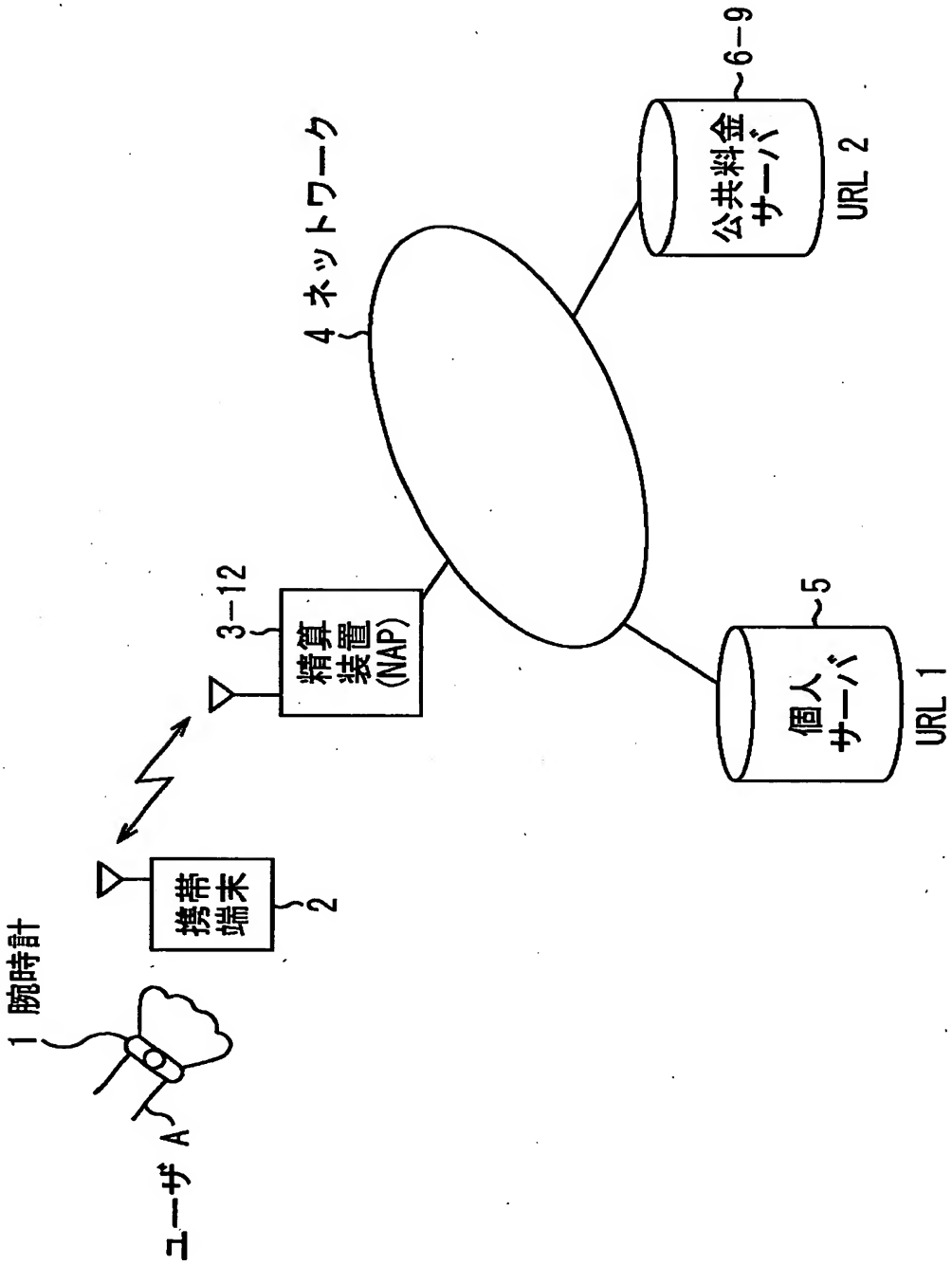
【図３３】


4 ネットワーク
6-8
通行料金サーバ
URL 2
3-11
料金ゲート機(NAP)
3-10
入門ゲート機(NAP)
5
個人サーバ
URL 1
1 腕時計
2
携帯端末
ユーザ A
自動車 A

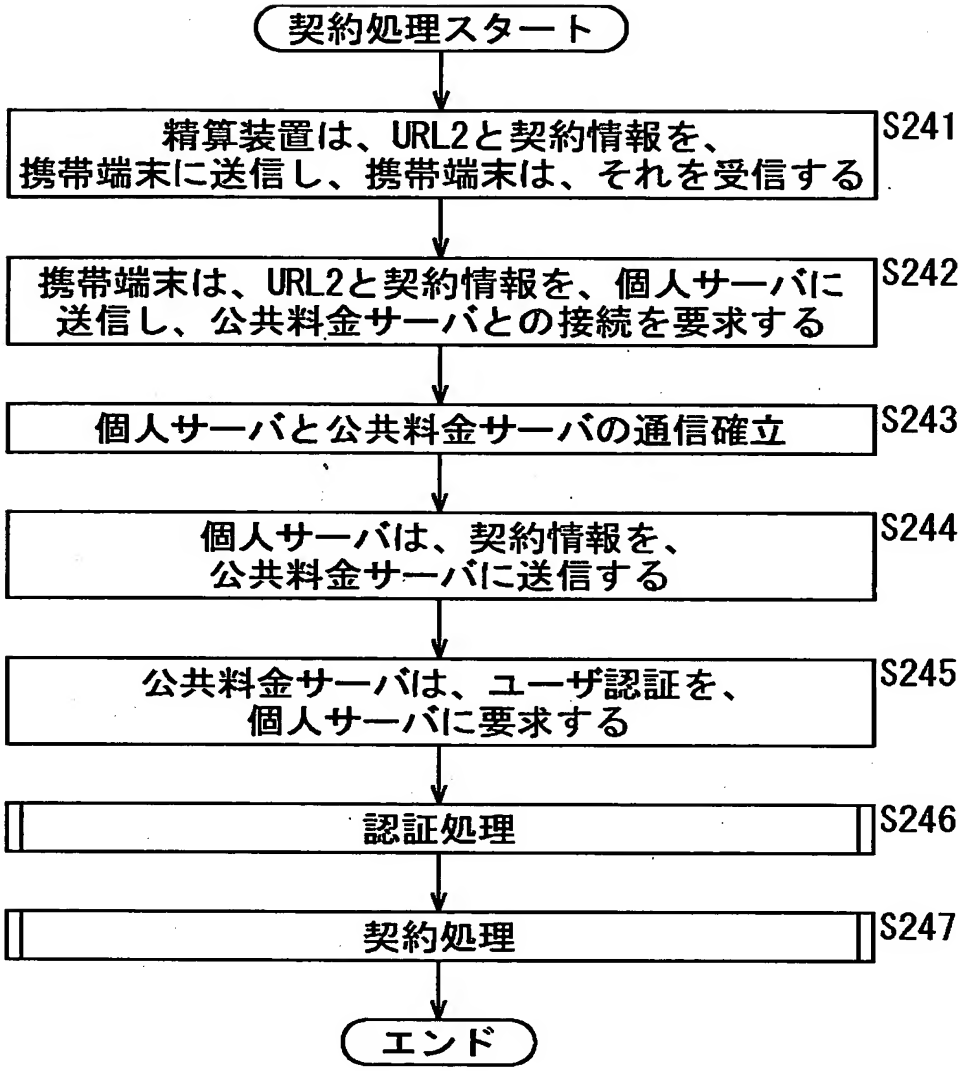
【図３４】


有料道路の料金自動支払処理スタート
携帯端末は、URL1を、入門ゲートに送信し、
入門ゲートは、それを受信する
S221
入門ゲートは、URL1とその受信時刻を、
通行料金サーバに送信し、
通行料金サーバは、それを受信する
S222
通行料金サーバは、URL1とその受信時刻を記憶する
S223
携帯端末は、URL1を、料金ゲートに送信し、
料金ゲートは、それを受信する
S224
料金ゲートは、URL1、受信時刻、車両番号を、
通行料金サーバに送信し、
通行料金サーバは、それを受信する
S225
登録された車両？
S226
NO
YES
支払処理
S227
処理
S228
エンド

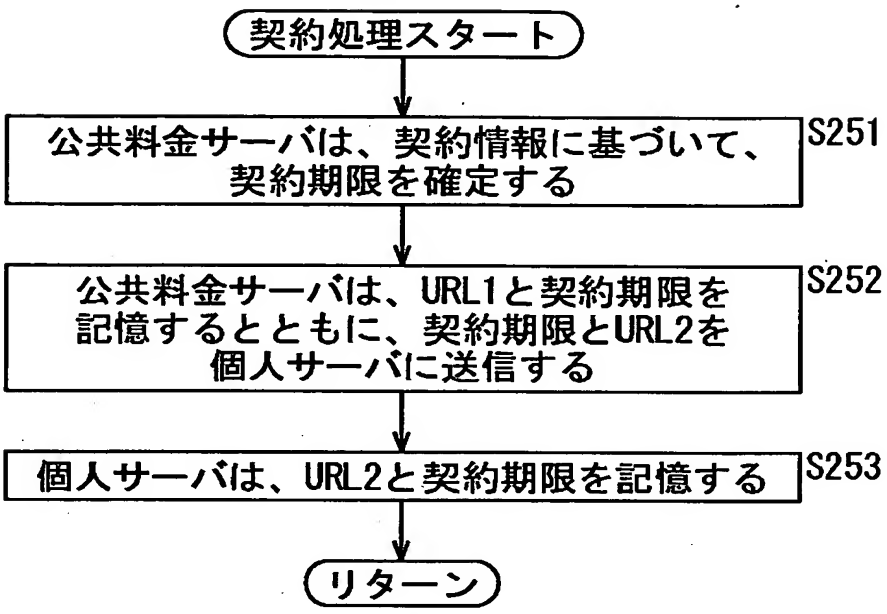
【図３５】


1 腕時計
ユーザ A
携帯端末
2
3-12
精算装置(NAP)
4 ネットワーク
5
個人サーバ
URL 1
6-9
公共料金サーバ
URL 2

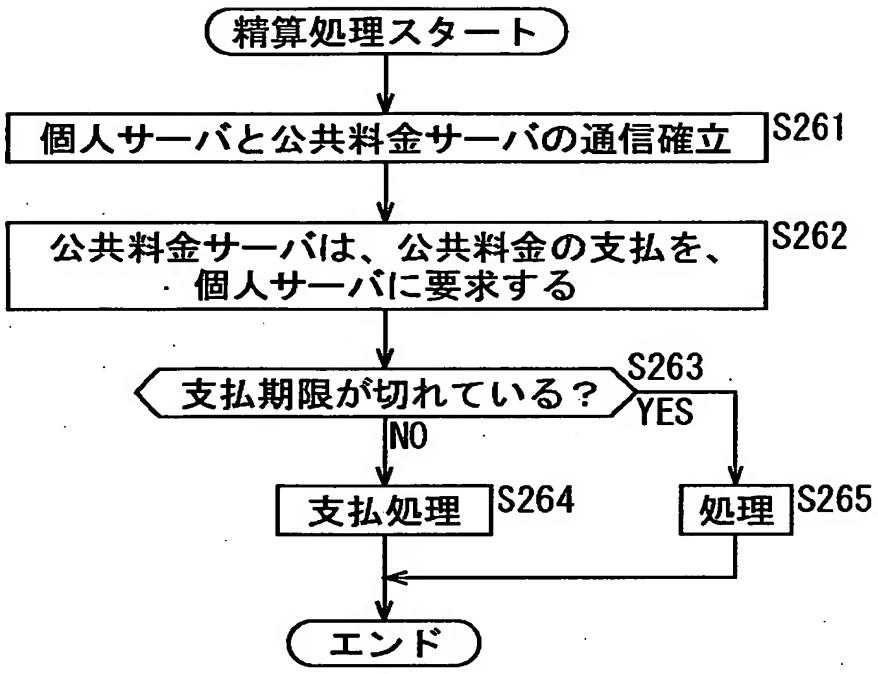
【図３６】


契約処理スタート
精算装置は、URL2と契約情報を、携帯端末に送信し、携帯端末は、それを受信する
S241
携帯端末は、URL2と契約情報を、個人サーバに送信し、公共料金サーバとの接続を要求する
S242
個人サーバと公共料金サーバの通信確立
S243
個人サーバは、契約情報を、公共料金サーバに送信する
S244
公共料金サーバは、ユーザ認証を、個人サーバに要求する
S245
認証処理
S246
契約処理
S247
エンド

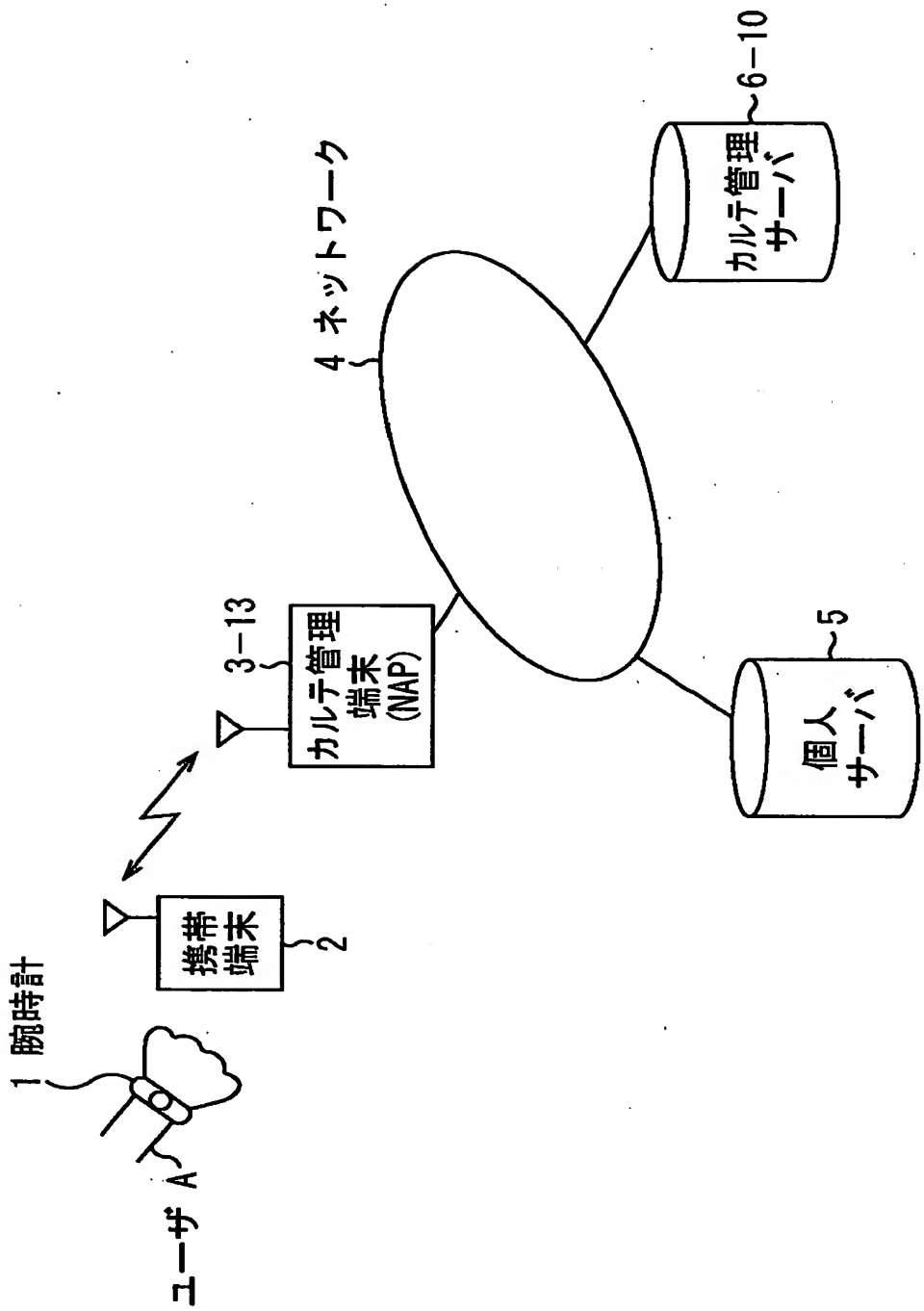
【図３７】


契約処理スタート
公共料金サーバは、契約情報に基づいて、契約期限を確定する
S251
公共料金サーバは、URL1と契約期限を記憶するとともに、契約期限とURL2を個人サーバに送信する
S252
個人サーバは、URL2と契約期限を記憶する
S253
リターン

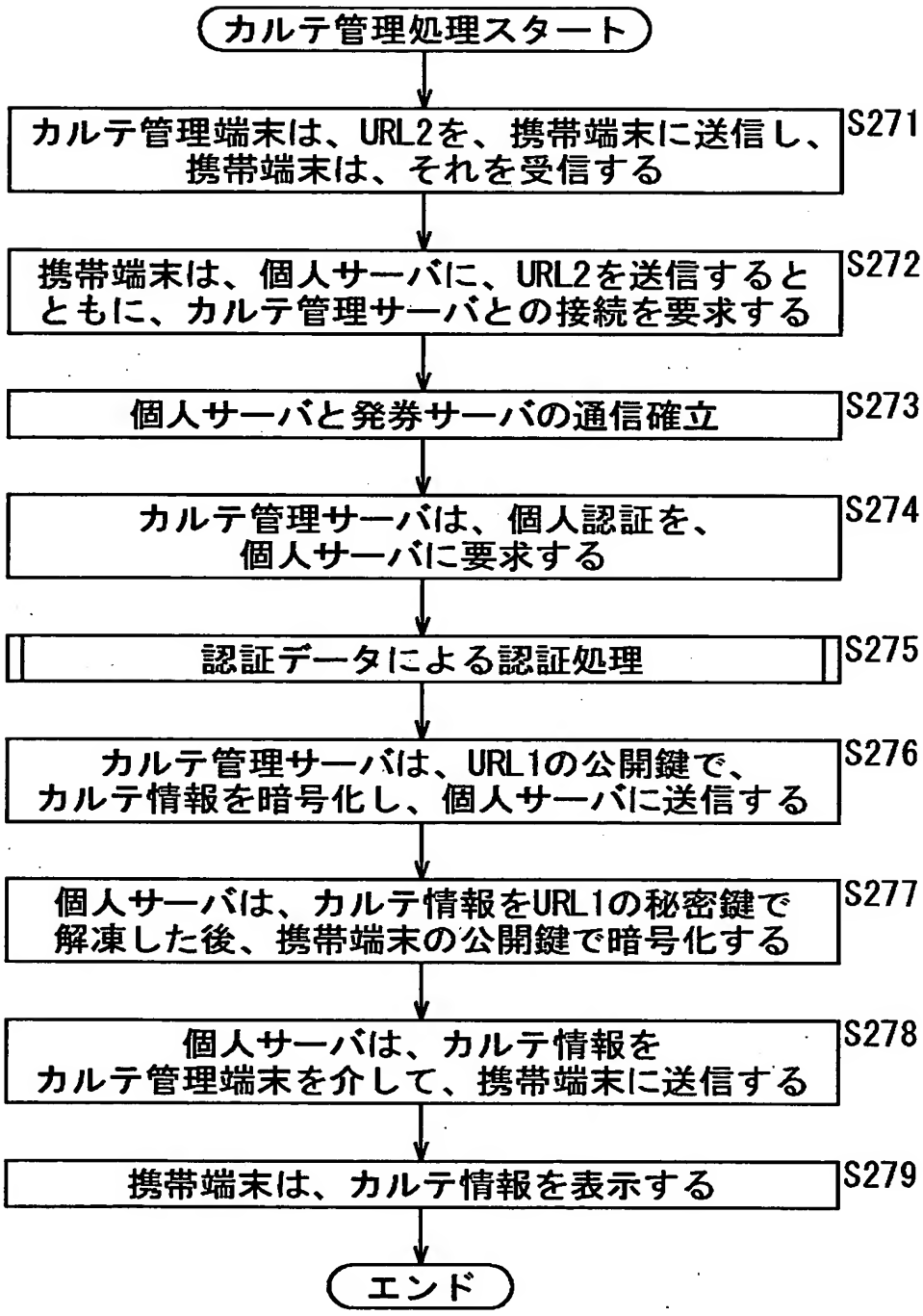
【図３８】


精算処理スタート
個人サーバと公共料金サーバの通信確立
S261
公共料金サーバは、公共料金の支払を、個人サーバに要求する
S262
支払期限が切れている？
S263
YES
NO
支払処理
S264
処理
S265
エンド

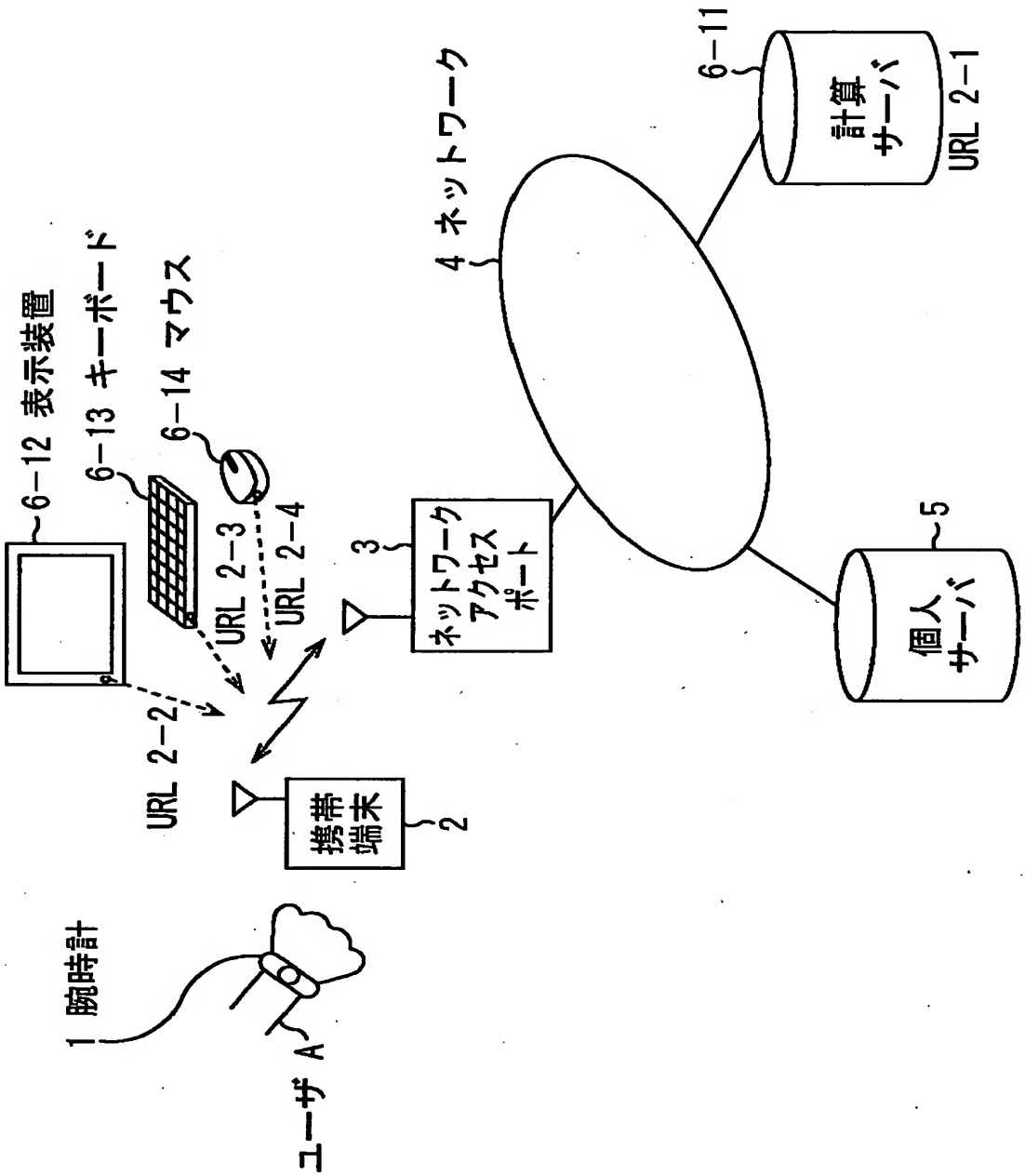
【図３９】


ユーザ A
1 腕時計
携帯端末
2
3-13
カルテ管理端末(NAP)
4 ネットワーク
5
個人サーバ
6-10
カルテ管理サーバ

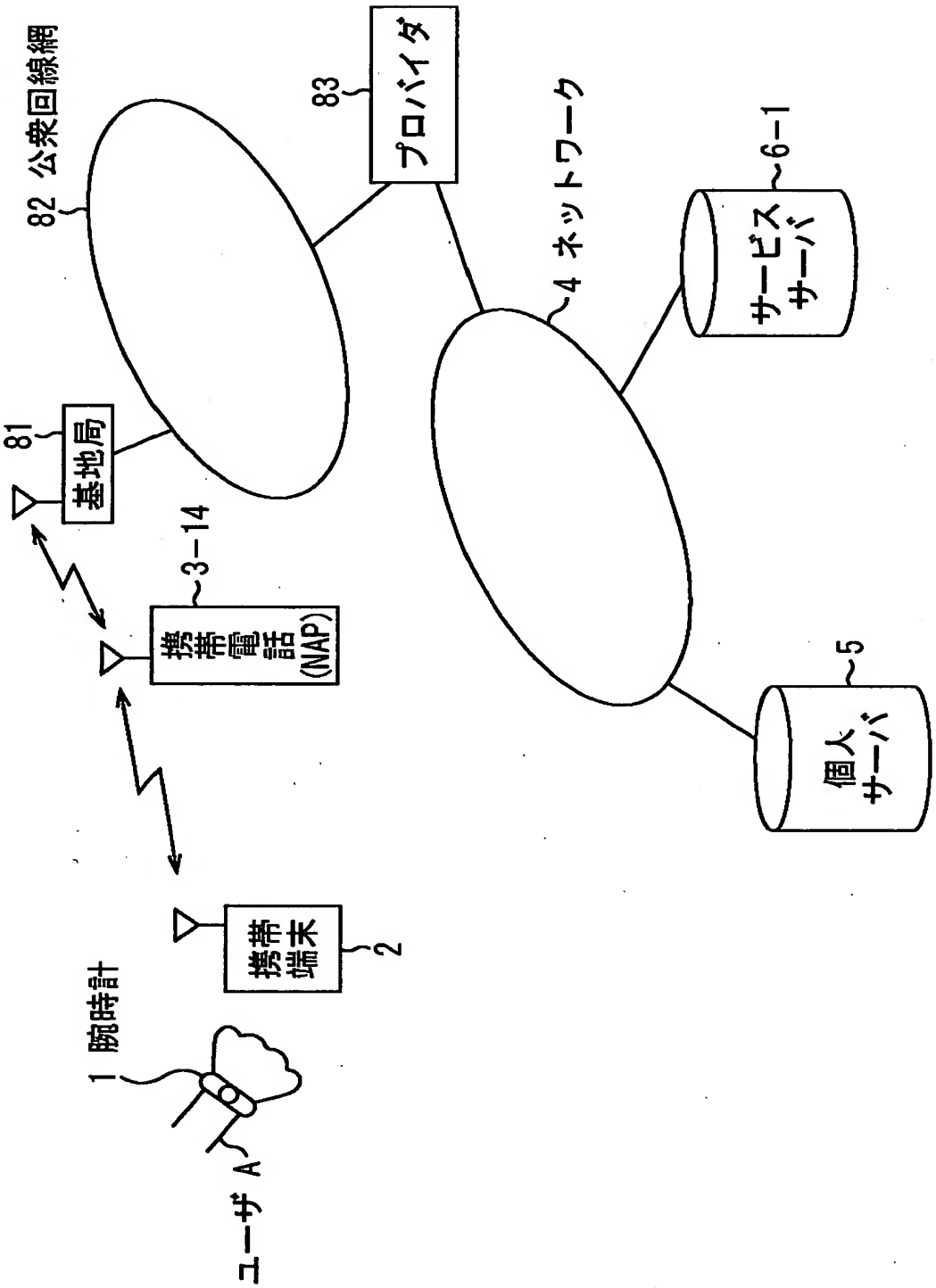
【図４０】


カルテ管理処理スタート
カルテ管理端末は、URL2を、携帯端末に送信し、携帯端末は、それを受信する
S271
携帯端末は、個人サーバに、URL2を送信するとともに、カルテ管理サーバとの接続を要求する
S272
個人サーバと発券サーバの通信確立
S273
カルテ管理サーバは、個人認証を、個人サーバに要求する
S274
認証データによる認証処理
S275
カルテ管理サーバは、URL1の公開鍵で、カルテ情報を暗号化し、個人サーバに送信する
S276
個人サーバは、カルテ情報をURL1の秘密鍵で解凍した後、携帯端末の公開鍵で暗号化する
S277
個人サーバは、カルテ情報をカルテ管理端末を介して、携帯端末に送信する
S278
携帯端末は、カルテ情報を表示する
S279
エンド

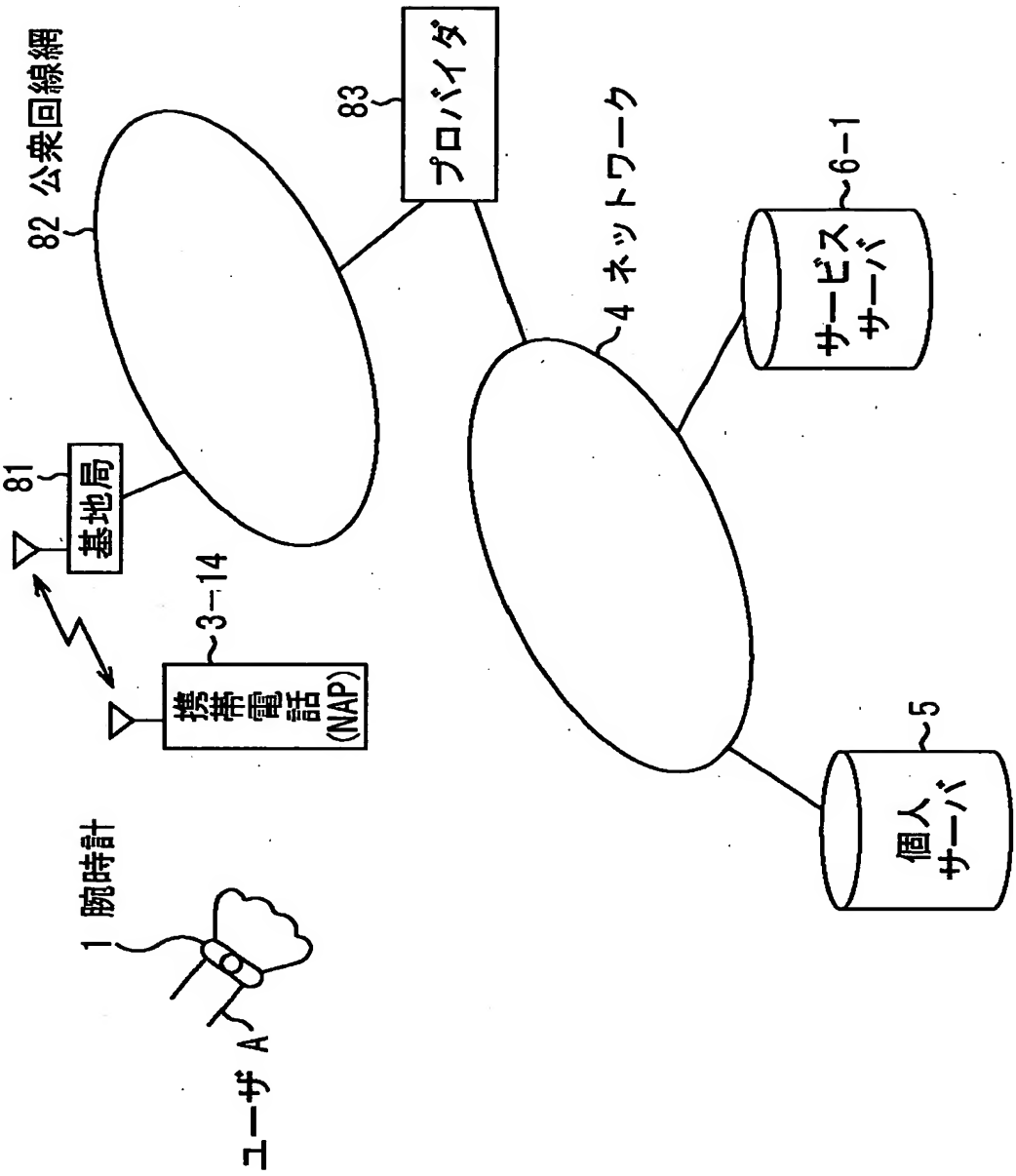
【図４１】


1 腕時計
ユーザ A
携帯端末
2
URL 2-2
URL 2-3
URL 2-4
6-12 表示装置
6-13 キーボード
6-14 マウス
3
ネットワークアクセスポート
4 ネットワーク
6-11
計算サーバ
URL 2-1
5
個人サーバ

【図４２】


1 腕時計
ユーザ A
2 携帯端末
3-14 携帯電話 (NAP)
81 基地局
82 公衆回線網
83 プロバイダ
4 ネットワーク
5 個人サーバ
6-1 サービスサーバ

【図４３】


1 腕時計
ユーザ A
3-14
携帯電話 (NAP)
81
基地局
82 公衆回線網
83
プロバイダ
4 ネットワーク
6-1
サービス サーバ
5
個人 サーバ

【書類名】　　要約書

【要約】

【課題】　個人情報を保持しない携帯端末で、サービス提供システムを利用することができるようにする。

【解決手段】　腕時計１は、パスワードを発生する。携帯端末２は、個人サーバ５に記憶されているユーザＡの個人情報を指定するＵＲＬ１を記憶しており、そのＵＲＬ１を、精算装置３－１に送信する。精算装置３－１は、携帯端末２に対するネットワークアクセスポートとしての役割を果たす。個人サーバ５は、ＵＲＬ１により特定される、ユーザＡの個人データを管理するサーバであり、ネットワーク４を介して、精算装置３－１やサービスサーバ６－１と通信する。サービスサーバ６－１は、ＵＲＬ２により特定される処理をサーバである。サービスサーバ６－１が、その処理を、ネットワーク４を介して、精算装置３－１や個人サーバ５と通信して実行する。これにより、ユーザＡは、各種サービスの提供を受けることができる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
　［変更理由］　新規登録
　　住　所　　東京都品川区北品川６丁目７番３５号
　　氏　名　　ソニー株式会社

US 1003989405P1

Creation date: 09-10-2004
Indexing Officer: TBUI3 - TAI BUI
Team: OIPEBackFileIndexing
Dossier: 10039894

Legal Date: 05-14-2002

No.	Doccode	Number of pages
1	C.AD	1

Total number of pages: 1

Remarks:

Order of re-scan issued on .....